

SUNIVERSITÀ DEGLI STUDI DI GENOVA

Faculty of Law

PhD in Security, Risk and Vulnerability

Curriculum Security and Law



PhD Thesis

A LEGAL PERSPECTIVE ON CYBERSECURITY BETWEEN EUROPEAN AND  
NATIONAL INTERVENTIONS

Supervisor

Prof. Francesca Bailo

PhD candidate

Fabio Gaggero

XXXVI PhD cycle

“If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology”

Bruce Schneier

To my family

To my teachers, both past  
and present

## I Abstract

Cybersecurity is a complex and multifaceted field that spans multiple sectors and disciplines, from technical domains to legal, governance and social aspects. With the emergence of new technologies, such as IoT and artificial intelligence, the challenges surrounding cybersecurity are becoming increasingly complex. This thesis examines the European and Italian regulatory frameworks for cybersecurity, focusing on how evolving European Union policies and regulations have shaped interventions at the national level. Through a historical and reconstructive approach, the research outlines the evolution of key European cybersecurity policies, highlighting the increasing complexity and fragmentation caused by overlapping regulations.

The study is divided into four main chapters. The first two examine the European framework, beginning with an analysis of EU cybersecurity policy and then presenting European legislative interventions in chronological order. These chapters categorise various regulatory initiatives and assess their impact on national legislation. The third chapter focuses on the Italian cybersecurity infrastructure, mapping its evolution. The final chapter addresses a grey area in the regulatory framework concerning constitutional bodies, using interviews to investigate the impact of national cybersecurity regulations on these institutions.

This research, conducted in collaboration with the ERACLITO project, contributes to the academic debate on cybersecurity regulation by mapping compliance requirements at both European and national levels. The appendices provide additional technical details, including a functional standard for security requirements within the ERACLITO project, ensuring that the technical content does not overwhelm the core analysis.

## II Contents

|           |                                                                                    |     |
|-----------|------------------------------------------------------------------------------------|-----|
| I         | Abstract                                                                           | I   |
| II        | Contents                                                                           | II  |
| III       | Table of figures                                                                   | IV  |
| I         | Introduction to the cybersecurity realm: narrowing the scope                       | 1   |
| II        | European Cybersecurity Policies                                                    | 7   |
| II.1      | The nineties: security as standardization                                          | 11  |
| II.2      | The new millennium: security as a reaction to threats                              | 18  |
| II.2.1    | eEurope 2002 strategy (1999-2002)                                                  | 18  |
| II.2.2    | eEurope 2005 strategy (2002-2005)                                                  | 25  |
| II.2.3    | i2010 strategy (2005-2010)                                                         | 28  |
| II.3      | Ten years to the present: from the failure of the strategy to modern cybersecurity | 36  |
| II.3.1    | Europe 2020                                                                        | 38  |
| II.3.2    | The 2013 Cybersecurity Strategy                                                    | 42  |
| II.3.3    | The update of the strategy                                                         | 52  |
| II.3.4    | The last EU cybersecurity strategy                                                 | 58  |
| III       | EU legislation about cybersecurity                                                 | 64  |
| III.1     | Regulations related to cybersecurity                                               | 65  |
| III.1.1   | Electronic communications' framework                                               | 66  |
| III.1.1.1 | Continuation regarding the security aspects                                        | 71  |
| III.1.2   | Defining "privacy" and getting to know the underlying complexity                   | 79  |
| III.1.2.1 | GDPR: an excerpt from the point of view of Cybersecurity                           | 86  |
| III.1.2.2 | Privacy in the field of electronic communications                                  | 94  |
| III.1.3   | Critical infrastructures                                                           | 97  |
| III.1.3.1 | Origins and the European debate                                                    | 97  |
| III.1.3.2 | The first directive on critical infrastructures                                    | 101 |
| III.1.3.3 | The new European Critical Infrastructures directive                                | 109 |
| III.2     | The NIS Framework                                                                  | 113 |
| III.2.1   | The first NIS directive                                                            | 118 |
| III.2.2   | The NIS reform                                                                     | 127 |
| IV        | The Italian Cybersecurity Perimeter                                                | 141 |
| IV.1      | The Perimeter before the Perimeter                                                 | 142 |
| IV.1.1    | History and foundations of the Italian secret service system                       | 144 |
| IV.1.2    | The law n. 124 of 2007                                                             | 148 |
| IV.1.3    | Reforms and amendments to Law 124 of 2007                                          | 154 |

|        |                                                                                                        |       |
|--------|--------------------------------------------------------------------------------------------------------|-------|
| IV.1.4 | Il D.P.C.M. 24 January 2013 (Monti's decree)                                                           | 158   |
| IV.1.5 | Il D.P.C.M. 17 February 2017 (Gentiloni's decree)                                                      | 162   |
| IV.2   | The structure of the Perimeter                                                                         | 167   |
| V      | Direct Insights into the Cybersecurity Perimeter of Constitutional Bodies: A Questionnaire-based Study | 179   |
| V.1    | The experimental activity                                                                              | 181   |
| V.1.1  | The Agreements                                                                                         | 183   |
| V.1.2  | Adaptation to the technological standard                                                               | 183   |
| V.1.3  | The security organisation                                                                              | 188   |
| VI     | An ongoing conclusion                                                                                  | 192   |
| I      | Appendix I - Compliance for the Perimeter Subjects                                                     | i     |
| I.1    | Some basic concepts about standards and guidelines                                                     | i     |
| I.2    | What is a management system: an example from ISO 27001                                                 | vi    |
| I.3    | Other ISOs related to information security                                                             | xvi   |
| I.4    | The NIST cybersecurity framework                                                                       | xxiv  |
| I.5    | A Brief History of the Italian National Cybersecurity Framework                                        | xxxii |
| I.6    | Compliance requirements from the Italian Cybersecurity Perimeter                                       | xxxvi |
| II     | Appendix II – Mapping of the European legislation about cybersecurity                                  | liii  |
| III    | Appendix III – Table of main findings from European legislation                                        | liv   |
| IV     | Appendix – Key sources of national law for the National Cybersecurity Perimeter                        | lxii  |
| V      | References                                                                                             | lxiv  |

### III Table of figures

|                                                                                                  |        |
|--------------------------------------------------------------------------------------------------|--------|
| Figure 1 - Categories of EU policies about cybersecurity                                         | 63     |
| Figure 2 - Security measures domains concerning EEC                                              | 75     |
| Figure 3 - Incident notification according to EEC                                                | 78     |
| Figure 4 Data protection regulations and cybersecurity's overlapping                             | 81     |
| Figure 5 - DPIA procedure according to GDPR                                                      | 91     |
| Figure 6 - Data breach notification procedure in the light of GDPR                               | 92     |
| Figure 7 - Data breach notification according to regulation 611/2013                             | 96     |
| Figure 8 - Scope of the first Critical Infrastructures Directive (Council Directive 2008/114/EC) | 103    |
| Figure 9 - Summary of the first Critical Infrastructures directive                               | 104    |
| Figure 10 - Concept of European Critical Infrastructure between different European countries     | 106    |
| Figure 11 - European Critical Infrastructures' sectors                                           | 110    |
| Figure 12 - Scope of NIS1 Directive                                                              | 120    |
| Figure 13 - Criteria to identify incidents' critical impact                                      | 123    |
| Figure 14 - Incident notification according to NIS1                                              | 124    |
| Figure 15 - NIS bodies in the NIS notification procedure                                         | 125    |
| Figure 16 - Scope of NIS2 directive                                                              | 133    |
| Figure 17 - Incident notification procedure according to NIS2                                    | 138    |
| Figure 18 - Summary of the NIS2                                                                  | 139    |
| Figure 19 - Italian Intelligence before Law n. 124/2007                                          | 148    |
| Figure 20 - Italian Intelligence after Law n. 124/2007                                           | 153    |
| Figure 21 - The Italian Cybersecurity Framework (D.P.C.M. Monti)                                 | 162    |
| Figure 22 - The Italian Cybersecurity Framework after D.P.C.M. Gentiloni                         | 165    |
| Figure 23 - The Italian Cybersecurity Framework after NIS transposition                          | 167    |
| Figure 24 - National Cybersecurity Perimeter's foundations                                       | 177    |
| Figure 25 - Standardisation Bodies                                                               | v      |
| Figure 26 - Standardisation common procedure                                                     | vi     |
| Figure 27 - Deming Cycle                                                                         | viii   |
| Figure 28 - ISO 27001 through the stages of the Deming Cycle                                     | ix     |
| Figure 29 - Risk Management process                                                              | xii    |
| Figure 30 - Risk assessment process                                                              | xiv    |
| Figure 31 - ISO 27000 family                                                                     | xvi    |
| Figure 32 - ISO 27000 family - Information Security Management                                   | xviii  |
| Figure 33 - ISO 27000 family - Other general guidelines                                          | xix    |
| Figure 34 - ISO 27000 family - Security in Specific Sectors                                      | xx     |
| Figure 35 - ISO 27000 family - Safeguarding ICT Continuity and Supplier Relationships            | xxi    |
| Figure 36 - ISO 27035 - Incident Management Cycle                                                | xxiii  |
| Figure 37 - ISO 27000 family - Digital Evidence and Incident Management                          | xxiv   |
| Figure 38 - NIST 2.0 Cybersecurity Framework - Functions, Categories, Subcategories              | xxvii  |
| Figure 39 - NIST Cybersecurity Framework example                                                 | xxviii |
| Figure 40 - NIST Cybersecurity Framework - Tiers                                                 | xxx    |
| Figure 41 - Italian Cybersecurity Framework - Components                                         | xxxiii |
| Figure 42 - Gantt chart of European legislation relevant to cybersecurity                        | liii   |
| Figure 43 - Sources of the Italian Cybersecurity Framework before the establishment of the       |        |

National Cybersecurity Perimeter    lxii

Figure 44 - Italian Cybersecurity Framework after the establishment of the National  
Perimeter                      lxiii



## I Introduction to the cybersecurity realm: narrowing the scope<sup>1</sup>

Addressing an issue as complex and multifaceted as cybersecurity presents significant challenges, especially as the term has evolved to encompass a wide range of meanings<sup>2</sup>. On top of the already wide variety of technical domains, the introduction of new technologies, from IoT to artificial intelligence, has added further layers of complexity.

This increases exponentially when considering the cross-cutting impact of cybersecurity across different sectors, each of which views it from a different perspective and with its own specificities.

The CYBOK attempts to capture this diversity of issues and sectors involved in an attempt to define the boundaries of such a vast phenomenon. A total of 21 knowledge areas are identified, 17 of which can be grouped into several strictly technical areas dealing with the security of various assets, such as infrastructure, systems, software and platforms. These are then flanked by multiple categories relating to offensive and defensive operations, from incident management to malware<sup>3</sup>.

Although fewer in number, the remaining areas of knowledge are entirely dedicated to the social sciences and are characterised by an equally varied subdivision within them. Even leaving aside both the cyber-risk governance and human-risk aspects, there is still an extremely large legal area to be addressed. On the one hand, the authors of the paper distinguish the perennial problem of balancing fundamental rights and security. Even without enumerating other rights from our Constitutional Charter, the right to privacy alone could take too long to treat exhaustively. On the other hand, there is the issue of cybersecurity regulation and legislation, which is the subject of this thesis.

Even with this defined scope, fully addressing the detail presents challenges due to the multitude of possible perspectives. The first question to be answered is that of the level to be addressed.

From an international perspective, cybersecurity can be about combating online crime, or rather cybercrime, through international cooperation organisations and instruments<sup>4</sup>. The issue is closely intertwined with that of the regulation of cyberspace and the effectiveness of traditional instruments of international law<sup>5</sup>.

---

<sup>1</sup> Considering the rapid regulatory changes in the last period, this work can be considered as updated until May 2024.

<sup>2</sup> Alessandro Armando and Fabio Roli, 'Intelligenza Artificiale e "Cybersecurity". Fatti, Miti e Rischi', *Gnosis*, no. 2 (2019): 143–51. In defining their terms, AI and cybersecurity, the authors define both as suitcase expressions rich in multiple meanings.

<sup>3</sup> Awais Rashid et al., eds., *CyBOK - The Cyber Security Body of Knowledge*, 1.1.0, 2021, [https://www.cybok.org/media/downloads/CyBOK\\_v1.1.0.pdf](https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf).

<sup>4</sup> Murdoch Watney, 'The Way Forward in Addressing Cybercrime Regulation on a Global Level', *Journal of Internet Technology and Secured Transaction* 1, no. 3 (1 September 2012): 61–67, <https://doi.org/10.20533/jitst.2046.3723.2012.0009>; Stein Schjolberg and Solange Ghernaouti-Helie, 'A Global Treaty on Cybersecurity and Cybercrime - Second Edition 2011', 2011; Olena V. Sviatun et al., 'Combating Cybercrime: Economic and Legal Aspects', *Wseas Transactions on Business and Economics* 18 (2021), <https://doi.org/10.37394/23207.2021.18.72>; Artur Appazov, *Legal Aspects of Cybersecurity* (Copenhagen: Faculty of Law - University of Copenhagen, 2014), [https://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal\\_Aspects\\_of\\_Cybersecurity.pdf](https://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf).

<sup>5</sup> Abid Adonis, 'International Law on Cyber Security in the Age of Digital Sovereignty', *E-International*

Even at the regional level, several regulatory experiences can be described. From America to China, all countries have been confronted in recent years with the age-old problem of establishing rules to regulate their resilience<sup>6</sup>.

Not to be outdone, the European Union has taken a number of regulatory steps to address the issue. From a broader focus on digitalisation, cybersecurity has become a key building block for the European single market. Although the market continues to be the justification for much European legislation, the Union's external action is receiving increasing attention.

Also at the national level, the Italian legislator has recently intervened to restructure the national cybersecurity system, both to incorporate the directions of the European plan and to make cooperation between institutional actors more efficient.

This focus is not due to a lack of research interest but is a necessary choice to navigate the subject's fluid and varied nature, limiting the scope to European and national contexts. The methodology of the work is practical, shaped both by the questionnaires administered to the Constitutional bodies and by the participation in the ERACLITO project<sup>7</sup>, with the limitation due to the constitutional perspective of the research.

Thematic strands related to cybersecurity are evident in academic literature<sup>8</sup>, each

---

*Relations*, 2020, <https://www.e-ir.info/pdf/82169>; Abram Chayes and Antonia Handler Chayes, *The New Sovereignty* (Harvard University Press, 1995), <https://doi.org/10.4159/9780674029453>; Laura DeNardis, *The Global War for Internet Governance* (Yale University Press, 2014), <https://doi.org/10.12987/yale/9780300181357.001.0001>; Jack Goldsmith, 'Who Controls the Internet? Illusions of a Borderless World', *Strategic Direction* 23, no. 11 (23 October 2007), <https://doi.org/10.1108/sd.2007.05623kae.001>; Harold Hongju Koh et al., 'Why Do Nations Obey International Law?', *The Yale Law Journal* 106, no. 8 (June 1997): 2599, <https://doi.org/10.2307/797228>; Julia Pohle and Thorsten Thiel, 'Digital Sovereignty', *Internet Policy Review* 9, no. 4 (17 December 2020), <https://doi.org/10.14763/2020.4.1532>.

<sup>6</sup> National Institute of Standards and Technology, 'The NIST Cybersecurity Framework 2.0' (Gaithersburg, MD: National Institute of Standards and Technology, 26 February 2024), <https://doi.org/10.6028/NIST.CSWP.29>; Aimin Qi, Guosong Shao, and Wentong Zheng, 'Assessing China's Cybersecurity Law', *Computer Law & Security Review* 34 (1 September 2018), <https://doi.org/10.1016/j.clsr.2018.08.007>; Iqbal Ramadhan, 'ASEAN-China Cybersecurity Cooperation: Challenges and Opportunities', *Journal of Social and Political Sciences* 6 (27 October 2023): 1–10, <https://doi.org/10.31014/aior.1991.06.04.440>; Yohannes Eneyew Ayalew, 'The African Union's Malabo Convention on Cyber Security and Personal Data Protection Enters into Force Nearly after a Decade. What Does It Mean for Data Privacy in Africa or Beyond?', *EJIL:Talk! The Blog of the European Journal of International Law*, 1 January 2023, [https://www.academia.edu/103386834/The\\_African\\_Union\\_s\\_Malabo\\_Convention\\_on\\_Cyber\\_Security\\_and\\_Personal\\_Data\\_Protection\\_enters\\_into\\_force\\_nearly\\_after\\_a\\_decade\\_What\\_does\\_it\\_mean\\_for\\_Data\\_Privacy\\_in\\_Africa\\_or\\_beyond](https://www.academia.edu/103386834/The_African_Union_s_Malabo_Convention_on_Cyber_Security_and_Personal_Data_Protection_enters_into_force_nearly_after_a_decade_What_does_it_mean_for_Data_Privacy_in_Africa_or_beyond); Inter American Development Bank and Organization of American States, 'Cybersecurity: Are We Ready in Latin America and the Caribbean?', *IDB Publications*, 14 March 2016, <https://doi.org/10.18235/0006517>.

<sup>7</sup> ERACLITO is a project of the SPOKE 7 of the Next Generation EU project «Security and Rights in CyberSpace» (SERICS). The project is leaded by Consorzio Interuniversitario Nazionale per l'Informatica (CINI). The Eraclito project aims to make a strategic and tangible contribution to the modernisation of the nation itself, in terms of its cybersecurity posture and cyber risk management capabilities. The project intends to contribute to the state of the art of cybersecurity in terms of knowledge, techniques, methodologies and tools for cyber risk management, cyber threat detection and hunting, and tools for managing the cybersecurity knowledge base, with respect to national (i.e. Perimetro di Sicurezza Nazionale Cibernetica) and European (i.e. Cybersecurity Act) regulations.

<sup>8</sup> A quick review of the scientific literature can be carried out using the DoGi search engine provided by the CNR (National Research Council or in Italian, Consiglio Nazionale delle Ricerche). At the time of writing, a search on the keyword "cybersecurity" returned 130 results. A selection led to the inclusion of only 74 papers, grouped

---

by topic. The diversity of the debates demonstrates the transversal nature of cybersecurity.

1) The relationship between data protection and cybersecurity. The main overlapping rules and specificities of the two frameworks are described in order to highlight possible synergies. On the other hand, the authors discuss the difficult balance between fundamental rights and security. See Mauro Alberto Brignoli, 'Analisi e Studio Di Una Soluzione Innovativa a Complemento Del GDPR per Promuovere La Cultura Della Sicurezza Informatica in Europa', *Cyberspazio e Diritto*, no. 1–2 (2018): 225–44; Tommaso Sica, "'Cybersecurity" e Governo Del Rischio', *Corporate Governance*, no. 4 (2022): 581–94; Federica Resta, 'Cybersicurezza e Protezione Dati: Un Rapporto Ambivalente', *Rivista Italiana Di Informatica e Diritto*, no. 2 (2024): 1; Benedetto Ponti, 'Il Rapporto Tra Cybersicurezza e Tutela Dei Dati Personali: Sinergie, Bilanciamenti e Parallelismi', *Rivista Italiana Di Informatica e Diritto*, no. 2 (2024): 2. Some case law of the European Court of Justice is recalled, in particular the Breyer and Tele2 Sverige v. Watson cases. See Marta Maurino, "'Cybersecurity", Sicurezza Nazionale e Trattamento Dei Dati Personali', *Amministrativ@mente*, no. 2 (2023): 939–72; Daniela Marrani, 'Cybersicurezza e Tutela Della Riservatezza Dei Dati Personali: Le Decisioni "Breyer" e "Tele2 Sverige" c. "Watson" Della Corte Di Giustizia UE', *Il Diritto Dell'Unione Europea*, no. 4 (2017): 791–827. Attention is also paid to some more sector-specific issues, such as the use of pseudonymisation techniques, appropriate security measures to complement Article 32 of the GDPR, or the protection of health data. See Sergio Guida, 'ENISA's Last Technical Analysis of Data Pseudonymization Advanced Measures in Data Protection and Privacy', *European Journal of Privacy Law & Technologies*, no. 1 (2021): 262–74; Alessandra Pietroletti and Alessandro Nicotra, 'Tutela Della Salute, Sistemi Digitali e Privacy', *Rivista Italiana Di Informatica e Diritto*, no. 1 (2022): 2\_283-294; Juan Sebastian Vanegas, 'La Violazione Dei Requisiti Di Sicurezza Informatica Di Cui All'articolo 32 Del GDPR', *Rivista Italiana Di Informatica e Diritto*, no. 2 (2020): 5–14.

2) Cybercrime in Italy and criminal investigations. A key issue is the legal development of cybercrime, particularly in Italy. Some specific crimes such as identity theft, phishing, malware attacks and social engineering are described. The literature emphasises the need for a harmonised legal framework to effectively combat cybercrime, and highlights the role of international cooperation in dealing with cross-border cybercrime. It also examines the challenge of attributing cyber attacks to specific actors, given the difficulty of prosecuting cyber crimes, which often transcend national borders. The literature also explores the role of public-private partnerships in the fight against cybercrime, in particular through information-sharing mechanisms designed to improve detection and prevention strategies. See Federica Montanaro, 'Il Bisogno Di Sicurezza Sulla Rete: L'intervento Penale Italiano Ed Europeo', *La Legislazione Penale*, no. 3 (2022): 3–14; Andrea Mattarella, 'Il "Cybercrime" Nell'ordinamento Italiano e Le Nuove Prospettive Dell'Unione Europea e Delle Nazioni Unite', *Diritto Penale e Processo*, no. 6 (2022): 809–29; Bianca Nicla Romano, 'Il Rischio Di "Attacchi" Ai Sistemi Informatici Tra Fattispecie Penalmente Rilevanti, Tutela Dei Dati Ed Esigenze Di "Buona Amministrazione"', *Amministrativ@mente*, no. 3 (2021): 545–94; Simone Bonavita, Alessandro Cortina, and Elisabetta Stringhi, "'Conosci Il Tuo Nemico": Un Primo Approccio Tassonomico Ai Principali Attacchi Informatici Nel Settore "Cybercrime" Bancario e Finanziario', *Cyberspazio e Diritto*, no. 3 (2020): 451–88; Pietro Maria Sabella, 'Il Fenomeno Del "Cybercrime" Nello Spazio Giuridico Contemporaneo. Prevenzione e Repressione Degli Illeciti Penali Connessi All'utilizzo Di Internet per Fini Di Terrorismo, Tra Esigenze Di Sicurezza e Rispetto Dei Diritti Fondamentali', *Informatica e Diritto*, no. 1–2 (2017): 139–76.

3) The relationship between AI and cybersecurity. Both the synergies and the new risks posed by AI are addressed. It examines the dual role of AI in enhancing cybersecurity and the potential vulnerabilities it introduces. If the automation of defensive cyber operations is made possible, AI can also be manipulated by attackers. A section of the literature examines the new risks posed by AI's generative capabilities, which can be exploited by attackers for more sophisticated spear-phishing or deepfakes. See Elisabetta Stringhi, 'La Minaccia Del "Deepfake" Ed i Rischi per La "Cybersecurity" Delle Organizzazioni Economiche: Un Approccio Pratico', *Cyberspazio e Diritto*, no. 1 (2021): 59–77; Barbara Poggiali, 'Le Opportunità Dell'Intelligenza Artificiale per La Sicurezza', *Gnosis*, no. 2 (2019): 135–41; Armando and Roli, 'Intelligenza Artificiale e "Cybersecurity". Fatti, Miti e Rischi'; Barbara Caputo, 'La Visione Computerizzata Dell'era Del "Deep Learning". Sfide e Opportunità per La "Cybersecurity"', *Gnosis*, no. 2 (2017): 90–95.

4) The international legal perspective on cybersecurity. The literature focuses on the application of international law to cyberspace, highlighting the challenges of attributing cyber attacks and enforcing legal responses. It discusses the need for international cooperation and new legal instruments to address cyber threats, with institutions such as the UN and NATO playing a key role in shaping global cybersecurity norms. Scholars also explore the legal complexities of cyber deterrence and retaliation, emphasising the importance of proportionate responses under international law. See Ranieri Razzante, 'L'attribuzione Degli Attacchi

---

Informatici', *European Journal of Privacy Law & Technologies*, no. 2 (2022): 0\_215-241; Wolfgang Kleinwächter, 'Wanted: Nobel Peace Prize Winners Who Create Peace in Cyberspace', *Rivista Italiana Di Informatica e Diritto*, no. 1 (2022): 1\_25-29; Giovanna Adinolfi, 'States' Economic Measures to Counter Cyberattacks: Disentangling Their (Il)Legitimacy under International Law', *Rivista Di Diritto Internazionale Privato e Processuale*, no. 3 (2022): 513-30. In addition, the concept of cyber sovereignty and the role of frameworks such as the Tallinn Manual in guiding state behaviour in cyber conflict are central to the debate. See Alessandra Sardu, 'L''international Cybersecurity Law': Lo Stato Dell'arte', *La Comunità Internazionale*, no. 1 (2020): 5-42.

5) Cybersecurity and public procurement. The literature examines how cybersecurity is integrated into public procurement processes. The evolving legal framework, including recent updates to Italian procurement laws, reflects the growing importance of integrating cybersecurity as a key criterion in public sector contracts. National strategic assets, such as 5G networks, are still subject to the Golden Power regulation. See Lorenzo Nannipieri, 'Cybersicurezza e Appalti Pubblici: Verso Un Nuovo (e Incerto) Quadro Regolatorio', *Rivista Italiana Di Informatica e Diritto*, no. 1 (2024): 19-23; Tommaso Cocchi, 'La Cybersicurezza Nel Prisma Del Diritto Dei Contratti Pubblici: Un Tentativo Di Ricostruzione Delle Regole Del Gioco Tra Requisiti Di Partecipazione, Criteri Di Aggiudicazione Ed Esigenze Di Certezza', *Munus*, no. 1 (2024): 177-207.

6) EU cyber-resilience legal interventions. This strand of literature focuses on the development of European cyber resilience legislation. The main themes are the updating of the NIS Directive and the introduction of other specific measures such as the Cyber Resilience Act (CRA) and the Digital Operational Resilience Act (DORA). See Giovanni Barbara, 'La "Cybersecurity": Minacce, Evoluzione Normativa, "Corporate Governance" e Nuove Prospettive', *Corporate Governance*, no. 4 (2022): 501-24; Flavia Bavetta, 'Direttiva NIS 2: Verso Un Innalzamento Dei Livelli Di Cybersicurezza a Livello Europeo - NIS', *MediaLaws*, no. 3 (2022): 405-14; Giulia Schneider, 'La Resilienza Operativa Digitale Come Materia Di "Corporate Governance": Prime Riflessioni a Partire Dal DORA', *Corporate Governance*, no. 4 (2022): 553-80; Matteo Buffa, 'La Direttiva NIS II Cybersecurity in Europa: Tra Innovazione, Formazione e Diritto Vivente', *Democrazia e Diritti Sociali*, no. 1 (2023): 47-64; Pier Giorgio Chiara, 'Il "Cyber Resilience Act": La Proposta Di Regolamento Della Commissione Europea Relativa a Misure Orizzontali Di Cybersicurezza per Prodotti Con Elementi Digitali', *Rivista Italiana Di Informatica e Diritto*, no. 1 (2023): 143-53; Francesca Di Gianni, 'Un'Europa "Ciberresiliente": La Risposta Dell'Unione Europea Alle Minacce e Agli Attacchi Informatici', *Studi Sull'integrazione Europea*, no. 2 (2023): 399-424; Federico Serini, 'Il Sistema Europeo Di Cooperazione Informativa per Il Contrasto Alle Minacce Informatiche. Verso Una Definizione Di Cybersicurezza Integrata?', *MediaLaws*, no. 3 (2023): 144-87; Federico Serini, 'La Frammentazione Del Cyberspazio Mercologico Tra Certificazioni e Standard Di Cybersicurezza. Alcune Considerazioni Alla Luce Delle Discipline Europea e Italiana', *Rivista Italiana Di Informatica e Diritto*, no. 2 (2023): 41-76; Federica Casarosa, 'L'armonizzazione Degli Obblighi Di Notifica: Il DDL Cybersicurezza Fra La NIS 2', *Rivista Italiana Di Informatica e Diritto*, no. 1 (2024): 11-14; Giovanni Comandè and Federica Casarosa, 'Aspettando La NIS2 ["Network and Information Systems"]: Ovvero Il Diritto Privato Della "Cybersecurity"', *Il Diritto Dell'informazione e Dell'informatica*, no. 1 (2024): 29-53. Some authors explore the possibility of adopting innovative governance measures, such as legal sandboxes, to guide future European interventions. See Filippo Bagni, 'The Regulatory Sandbox and the Cybersecurity Challenge: From the Artificial Intelligence Act to the Cyber Resilience Act', *Rivista Italiana Di Informatica e Diritto*, no. 2 (2023): 201-17. The NIS discourse is approached from different perspectives, some of which are more sectoral, such as the critical infrastructure, healthcare or small and medium-sized enterprises. See Elena Kaiser, 'The New NIS II Directive and Its Impact on Small and Medium Enterprises (SMEs): Initial Considerations', *MediaLaws*, no. 1 (2023): 343-57.

7) The national development of the National Cybersecurity Perimeter. The literature analyses the infrastructure of the Perimeter and the new Cybersecurity Agency (ACN). The PSNC is framed as a key instrument in protecting the country from cyber threats, involving strict regulations for public and private sectors managing critical services. See Fabio Carchidi, 'Perimetro Di Sicurezza Nazionale Cibernetica, Dal d.l. 105/2019 Ai d.p.c.m. n. 131/2020 e n. 81/2021: La Sublimazione Delle Cc.Dd. "Information and Communication Technologies"', *Ambienteditto.it*, no. 3 (2021): 295-305; Filippo Lorè and Paolo Musacchio, '"Cybersecurity" e Protezione Dei Dati Personali Ai Tempi Dell'"accountability": Verso Un Cambio Di Prospettiva?', *Amministrativ@mente*, no. 1 (2021): 65-90; Manfredi Matassa, 'Una Strategia Nazionale a Difesa Del Cyberspazio', *P.A. Persona e Amministrazione*, no. 2 (2022): 625-53; Federico Serini, 'La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021', *Federalismi.it*, no. 12 (20 April 2022); Edoardo Raffiotta, 'Cybersecurity Regulation in the European Union and the Issues of Constitutional Law', *Rivista AIC*, no. 4 (30 September 2022), [https://www.rivistaaic.it/images/rivista/pdf/4\\_2022\\_01\\_Raffiotta.pdf](https://www.rivistaaic.it/images/rivista/pdf/4_2022_01_Raffiotta.pdf); Simone Poletti, 'La Sicurezza Cibernetica Nazionale Ed Europea, Alla Luce Della Creazione Del Perimetro Di Sicurezza Nazionale Cibernetica', *MediaLaws*, no. 2 (2023): 398-410. The creation of the Centro di Valutazione e Certificazione

addressing specific sectoral aspects. However, a comprehensive overview is often missing, leaving room for further exploration. This lack is exacerbated by the marked over-regulation of the European legislator, which has a cascading effect on the internal framework and makes it more complex. Paradoxically, as much as the interventions are aimed at better integration and homogenisation of the common market, they have the opposite effect. The European Commission's strategy, A Europe Fit for the Digital Age, has led to a significant increase in regulatory measures in areas such as cybersecurity, data protection, artificial intelligence (AI) and digital services. This regulatory explosion has created overlapping and sometimes conflicting obligations, resulting in a fragmented regulatory landscape. The resulting strict requirements for service providers and data controllers can be seen as a bureaucratic burden. The need to comply with multiple sets of rules could slow down innovation and limit the European Union's ability to adapt to technological change. This is not only a compliance problem, but also an enforcement problem, as different legislation leads to overlapping competences of different authorities<sup>9</sup>.

Against the background of a fragmented and evolving scenario, this research aims to contribute to the current debate by providing an insight into the main European cybersecurity interventions. The main approach is mainly historical and reconstructive, in order to understand the direction of the current policy of the European legislator.

The first two chapters are dedicated to the European framework. The first reconstructs the main European cybersecurity policies, following the different EU strategies that have succeeded each other. The research objective is to reconstruct the main set of European

---

Nazionale (CVCN) plays a central role in vetting ICT providers and ensuring compliance with national security standards, particularly in areas such as telecommunications and 5G networks. See Bruno Carotti, 'Sicurezza Cibernetica e Stato-Nazione', *Giornale Di Diritto Amministrativo*, no. 5 (2020): 629–41. The literature also emphasizes the public-private partnerships necessary to enforce these cybersecurity measures, highlighting the legal and operational challenges in coordinating between governmental bodies and private entities. The ACN is depicted as a key actor in enforcing the perimeter, but also the President of the Council of the Ministry keeps a central role in the system. See Marta Fernandes dos Santos and Alfonso Contaldo, 'L'agenzia per La Cybersicurezza Nazionale: Istituzione e Problematiche in Campo', *Rivista Amministrativa Della Repubblica Italiana*, no. 5–6 (2022): 2\_343–365; Stefano Rossa, 'Administrative Law Reflections on Cybersecurity and on Its Institutional Actors, in the European Union and Italy', *Italian Journal of Public Law*, no. 2 (2022): 426–50; Andrea Renzi, 'La Sicurezza Cibernetica: Lo Stato Dell'arte', *Giornale Di Diritto Amministrativo*, no. 4 (2021): 538–48.

8) Digital sovereignty. The literature highlights the evolving role of the State in the management of cybersecurity. The State is presented as a central actor in the coordination and implementation of cybersecurity policies, with the Italian government's efforts through bodies such as the National Agency for Cybersecurity (ACN) highlighted as crucial for the protection of both public and private infrastructures. See Alfonso Contaldo, 'L'attuazione Della "Cybersecurity" Nazionale: Un Difficile Esercizio Di Una Funzione Pubblica', *Lo Stato*, no. 21 (2023): 283–97; Tommaso F. Giupponi, 'Il Governo Nazionale Della Cybersicurezza', *Quaderni Costituzionali*, no. 2 (2024): 277–303; Lorenzo Moroni, 'La Governance Della Cybersicurezza a Livello Interno Ed Europeo: Un Quadro Intricato', *Federalismi.It*, no. 14 (2024): 179–97. This is not a passive regulatory role, as the security of cyberspace is part of the State's duty to protect the public good. Cybersecurity should be a non-excludable and non-rivalrous good that benefits society as a whole. From this perspective, the position of the State is also linked to the growing concept of digital sovereignty, where governments assert control over national cyberspace to protect their citizens and critical infrastructure from global cyber threats. See Raffaella Brighi, 'Vulnerabilità e Sicurezza: Un'analisi Informatico-Giuridica Di Concetti in Evoluzione', *Notizie Di Politeia*, no. 136 (2019): 35–45; Raffaella Brighi and Pier Giorgio Chiara, 'La Cybersecurity Come Bene Pubblico: Alcune Riflessioni Normative a Partire Dai Recenti Sviluppi Nel Diritto UE', *Federalismi.It*, no. 21 (8 September 2021): 18–42.

<sup>9</sup> Edoardo C. Raffiotta, 'Dalla "Self-Regulation" Alla "over-Regulation" in Ambito Digitale: Come (e Perché) Di Un Necessario Cambio Di Prospettiva', *Osservatorio Sulle Fonti*, no. 2 (2023): 255–59.

policies relevant to cybersecurity. The policies are presented chronologically, following the different periods of European integration. At the end of the chapter, an attempt is made to abstract the main categories of intervention.

On the basis of this ideal grouping, the second chapter, devoted to European legislation, is grafted on. The research objective is to identify the main groups of European regulations related to cybersecurity. The main interventions directly or indirectly related to cybersecurity are collected and presented graphically to highlight their succession over time. Only some of them are examined in order to show the main influences from the European level on the national institutional framework.

The third chapter focuses on the internal framework. The aim of the research is to reconstruct the internal cybersecurity infrastructure from its beginnings to the current Perimeter Regulation. The description makes use of some graphical representations to highlight the actors, the relationships and the exchange of information between them.

The fourth chapter examines a particular grey area left by the Perimeter, namely that of constitutional bodies. Although there are no sources on the subject, an experimental approach is attempted through interviews with the staff of the organs. The aim of the research is to clarify the position of the constitutional bodies with regard to the Perimeter, with a focus on identifying any potential tensions between the new regulatory framework and their status of autonomy and independence.

The normative reconstruction carried out in the second and third chapters is closely linked to the research work carried out within the ERACLITO project. For this reason, some of the contents refer directly to the project of which they represent the research contributions of the research group of the University of Genoa.

These parts are complemented by a series of appendices, designed both to streamline the main text and to separate more technical content for clarity. The appendix I.6 describes how a technical security standard works, in order to introduce the requisitioning mechanism that will be followed within the ERACLITO project. The aim of the project is to comprehensively map the compliance requirements arising from national legislation. The current version of the functional requirements derived from the Perimeter Specification is presented in the appendix I.

## II European Cybersecurity Policies

In a digital world, where every object is connected, complexity is not just the right word to refer to technology, but a new way to describe reality with its multiple layers<sup>10</sup>. Remote machines, Internet service providers, web applications are all subtle examples of this intricacy that revolves around a medium that is deeply changing human perception and tightly strengthening its dependency. “In this sense, ICTs are not merely re-engineering but actually re-ontologizing our world”<sup>11</sup>, reversing the scarcity of information to abundance<sup>12</sup>.

Considering the disruptive characteristic of digitization, the European Union started to perceive the need to find a new point of balance that could compromise on the creation of a single internal market in the light of fundamental rights. As it was for the right to privacy, which soon found its new declension in the right to data protection, an urgency for security also began to emerge.

If privacy had almost immediately received an intervention by national lawmakers<sup>13</sup> and by the European community<sup>14</sup>, an early concept of cybersecurity could only be identified through non-binding acts<sup>15</sup> or must be sought within other sectorial regulations, which accompanied digital transition.

---

<sup>10</sup> Craig McTaggart, ‘A Layered Approach to Internet Legal Analysis’, *McGill Law Journal* 48 (2003): 574–88. The author, researching a proposal for a regulatory approach to the Internet, identified four different technological layers: a physical layer, an operational layer, an application layer, and a content layer. The first is composed by equipment, like computers and devices, and networks, those pieces that allow users to connect. The second concerns what allows the functioning of the network itself, that are standards and protocols. The third encompasses all the client and server-side applications, that run both locally and remotely. The latter is simply an expression of the multiplicity of contents, continuously produced and exchanged over the Net.

<sup>11</sup> Luciano Floridi, *Information: A Very Short Introduction*, Very Short Introductions 225 (Oxford ; New York: Oxford University Press, 2010), 15. The author clearly describe the symbiotic relationship between people and society, thus that “profound change in our conception of what it means to be an agent and what sort of environment these new agents inhabit [...] that is happening [...] through a radical transformation of our understanding of reality and of ourselves”. For further insights, see also Luciano Floridi, *Infosfera: etica e filosofia nell'età dell'informazione*, Digitalica (Torino: Giappichelli, 2009); Luciano Floridi, *La quarta rivoluzione: come l'infosfera sta trasformando il mondo*, Scienza e idee (Milano: Cortina Raffaello, 2017).

<sup>12</sup> Luciano Floridi, *The Onlife Manifesto: Being Human in a Hyperconnected Era*, 2014, 43, <http://doi.org/10.1007/978-3-319-04093-6>.

<sup>13</sup> The first regional law about privacy and data protection was the law of the Land of Hesse and Bavaria in 1978, while the first national law was the Swedish *Datalagen* in 1973. Between the seventies and the eighties of the last century several other laws followed, like the American Privacy Act in 1974, the German *Bundesdatenschutzgesetz* (BDSG) in 1977, and the French *Loi relative à l'informatique, aux fichiers et aux libertés* during the same year. The last, just before the first European interventions, was the British Data Protection Act in 1984.

<sup>14</sup> The first and coherent intervention came with European Parliament and Council of the European Union, ‘Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data’ (1995), 46, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046>. Since this is not the place to discuss the development of the right to privacy in the European Union, I refer to Franco Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo*, Seconda ristampa, I diritti nella rete nella rete, 4.1 (Torino: G. Giappichelli, 2016), 64–67. For some comparison between cybersecurity and data protection see III.1.2.1.

<sup>15</sup> Thomas Christiansen and Christine Neuhold, ‘Informal Politics in the EU: Informal Politics in the EU’, *JCMS: Journal of Common Market Studies* 51, no. 6 (November 2013): 1196–1206, <https://doi.org/10.1111/jcms.12068>.

Obviously, this attempt to outline a history of cybersecurity must deal with at least a couple of problems that can only partially be mitigated. Therefore, it is necessary to address them before starting to describe the first European interventions.

The first one comes from the use of a changing terminology over time. This is a form of complexity that relies on the language evolution and adaptation. On the one hand, the global and massive diffusion of technology has fostered the birth of several local and approximate translations of the different terms used by computer science experts<sup>16</sup>. On the other hand, the branch of computer science studies concerning security has evolved alongside the progression of the expressions used to address it, from the early information security to the modern cybersecurity.

This is the proof of the inherently dynamic nature of cybersecurity. The rapid advancements in technology and the constant emergence of new threats require an equally agile response from lawmakers and security experts. Consequently, the policies and measures implemented to tackle cybersecurity issues have undergone continuous evolution, making it difficult to pinpoint definitive moments in its progression.

The second issue concerns the integration of the European market<sup>17</sup>, whose aim was to remove all obstacles to the internal movements. Since the establishment of the European Communities and then of the European Community with the Maastricht treaty in 1992, all

---

<sup>16</sup> As an example, I can recall here a brief comment on the decree 82/2021, that established the Italian Agency for National Cybersecurity. Although the author is a cybersecurity expert from a technical standpoint, his opinion very well underlines the ambiguous use of specific terminologies by the legislator because “5% of the text covers things like the Accademia della Crusca’s disquisitions on whether the term *cybersicurezza*, rather than *sicurezza cibernetica*, should be used, or the Italianized version *cibersicurezza*” [my translation]. Nicola Grandis, ‘Agenzia per la cyber security, accelerare su tecnologia, investimenti e conoscenze: ecco perché’, *Agenda Digitale*, 5 July 2021, <https://www.cybersecurity360.it/cybersecurity-nazionale/agenzia-per-la-cyber-security-accelerare-su-tecnologia-investimenti-e-conoscenze-ecco-perche/>. This allows also to highlight the lack of proper knowledge when translating a technical term. As the cited sentence reminds, cybersecurity is usually italianised with the word “*cibernetica*” that derives from the Greek κυβερνητική, meaning “governance”. The word had been first used by André-Marie Ampère in 1834 and was adopted by artificial intelligence scholars during the second half of the last century. After Norbert Wiener had used it to define that feature of machine that is able to act and react to external environmental stimuli in 1948, this theory converged into John McCarthy’s research, one of the fathers of artificial intelligence studies. This seems to be enough to prove the complete irrelevance of the term in the cybersecurity context. For further insights see Paolo Moro, ‘Macchine come noi. Natura e limiti della soggettività robotica’, in *Intelligenza artificiale: il diritto, i diritti, l’etica*, by Guido Alpa and Augusto Barbera, ed. Ugo Ruffolo, Tech e-Law (Milano: Giuffrè Francis Lefebvre, 2020), 48–52.

<sup>17</sup> The complexity of the European integration was naturally reflected on the technological development. For this reason, it is appropriate to briefly resume here the main steps of the European history, just to set some milestones that can help as a compass during further dissertation.

The first phase encompasses the establishment of the three European Communities, the European Coal and Steel Community (ECSC), created by the Treaty of Paris in 1952, the European Economic Community (EEC), the European Atomic Energy Community (Euratom), created by the Treaty of Rome in 1957. After the Merger Treaty in 1965 and the creation of common institutions for the three communities, the enlargement of the European project brought to the Schengen treaty in 1985.

Ideally a second phase can be outlined with the Maastricht treaty in 1992 that merged the EEC and ECSC into the European Community, whose term had been used for the first time. In addition, the treaty introduced a division of the functions in three main pillars: economy and common market, that were the object of the new European Community (first pillar), foreign policy and common security (second pillar), and police and judiciary cooperation in the criminal field (third pillar).

The last phase is marked by the Lisbon Treaty in 2007 that finally created the European Union, unifying all pillars that have just been recalled.



member states received a significant prompt to achieve the creation of “an internal market characterized by the abolition, as between Member States, of obstacles to the free movement of goods, persons, services and capital”<sup>18</sup>.

This push towards a common market also implied the introduction of policies with the purpose of supporting the liberalisation of the technologies that underlie the horizontal implementation of ICTs. Although technology may be deemed as a supranational phenomenon detached from each single national set of rules, it is a multi-layered and integrated system of providers and infrastructures that cross different territories. For this reason, the spread of the Internet did not happen without the intervention of the European lawmaker, who had to set an essential approximation between national legislations, whose milestone can be found in the Green Paper released by the European Commission in 1987<sup>19</sup>. The publication of that book was a decisive event for the development of information technology in Western Europe and for its legal framing in national and EU legislation<sup>20</sup>.

Following the release of the Green Paper in 1987, the European Commission continued to play a pivotal role in shaping the legal landscape surrounding information and communication technologies (ICTs) within the European Union. As ICTs continued to evolve at a rapid pace, the need for harmonization and coherence among member states became increasingly evident. Consequently, the European Commission strived to create a unified legislative framework that would address the challenges posed by the ever-evolving digital environment and promote a seamless integration of ICTs across the region.

The passage from a fragmented situation to the unlocking of the real networking’s potential was marked by the implementation of some directives and decisions during the end of the 1980s, when “telecommunications [were], either wholly or partly, a State monopoly generally granted in the form of special or exclusive rights to one or more bodies responsible for providing and operating the network infrastructure and related services”<sup>21</sup>. In that condition, challenging the special rights related to terminal equipment exercised by national

---

<sup>18</sup> See art. 3 let. c) of the Maastricht treaty of 1992.

<sup>19</sup> See European Commission, ‘Towards a Dynamic European Economy, Green Paper on the Development of the Common Market for Telecommunications Services and Equipment’, 30 June 1987, COM/87/290FINAL, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:51987DC0290>.

<sup>20</sup> Notwithstanding the crucial importance of this moment, which was one of the first European approaches to the information society, it must be emphasised how late Europe's response to the digital revolution was, especially when compared with the policies of individual Member States or other non-EU countries. Without taking the easy example of the USA, which is undoubtedly the home of the Internet and IT, it is possible to recall the Japanese experience of early digitisation in the 1960s. While in the western world information technologies were first used by the military, “the Japanese Ministry of Industry and International Trade began implementing programs known as “Technopolis” and “Teletopia”, which aimed at connecting several Japanese cities and rural areas with electronic communication networks and transferring the work of administration, business, and citizens to the network”. See Centre for Europe, University of Warsaw, Poland and Marta Grabowska, ‘Legal, Political and Organizational Aspects of Cybersecurity in the European Union’, *On-Line Journal Modelling the New Europe*, no. 38 (9 April 2022): 108, <https://doi.org/10.24193/OJMNE.2022.38.05>. This endeavour soon became a research object for France, which was searching for the right approach to tackle the incoming information society during the late seventies. See Simon Nora and Alain Minc, ‘L’informatisation de la société rapport a M.le Président de la République’ (Paris, January 1978), [https://medias.vie-publique.fr/data\\_storage\\_s3/rapport/pdf/154000252.pdf](https://medias.vie-publique.fr/data_storage_s3/rapport/pdf/154000252.pdf).

<sup>21</sup> See Council of the European Communities, ‘Commission Directive 88/301/EEC of 16 May 1988 on Competition in the Markets in Telecommunications Terminal Equipment’, Pub. L. No. 301, EEC (1988), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31988L0301>.

monopolies was the first necessary step to enforce competition. As a result, harmonized standards for terminal equipment were introduced to guarantee uniform communication between member states<sup>22</sup>.

While this intervention only concerned terminal equipment, another important passage in this evolution of the electronic communications framework was the Open Network Provision (ONP)<sup>23</sup>, which established an open market for electronic communication services through the harmonization of conditions for open and efficient access, followed by a specific arrangement to ensure competition within it<sup>24</sup>.

These interventions occurred alongside the progressive development of the single market, which was beginning to recognize the opportunities possible through exploiting data. An example of this inherent tendency can be seen in the TEDIS (Trade Electronic Data Interchange System) European program<sup>25</sup>, whose purpose was to promote the creation of a common standard to exchange trade electronic data, while also addressing the legal issues that were inhibiting the development of this interchange, potentially amending national restrictive telecommunications regulations.

All these requirements enabled the emergence of a new market of informatics, “[...] a new market system unknown in previous ages, conditioned precisely by automated information, but limited and restrained by the monopolistic or oligopolistic positions of state-owned enterprises, which contradicted the fundamental principle of freedom of competition, communication, and exchange. [...] The European common market represents the new economic, legal and technical reality in which the start of a free movement of information technology goods and telematics services occurs”<sup>26</sup>.

The following paragraphs will attempt to explain the development of digital in Europe,

---

<sup>22</sup> See Council of the European Communities, ‘Council Directive 86/361/EEC of 24 July 1986 on the Initial Stage of the Mutual Recognition of Type Approval for Telecommunications Terminal Equipment’, Pub. L. No. 361, EEC (1986), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31986L0361>; Council of the European Communities, Commission Directive 88/301/EEC of 16 May 1988 on competition in the markets in telecommunications terminal equipment; Council of the European Communities, ‘Council Directive 91/263/EEC of 29 April 1991 on the Approximation of the Laws of the Member States Concerning Telecommunications Terminal Equipment, Including the Mutual Recognition of Their Conformity’, Pub. L. No. 263, EEC (1991), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31991L0263>.

<sup>23</sup> See Council of the European Communities, ‘Council Directive 90/387/EEC of 28 June 1990 on the Establishment of the Internal Market for Telecommunications Services through the Implementation of Open Network Provision’, Pub. L. No. 387, EEC (1990), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31990L0387>.

<sup>24</sup> See European Commission, ‘Commission Directive 90/388/EEC of 28 June 1990 on Competition in the Markets for Telecommunications Services’, Pub. L. No. 388, EEC (1990), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31990L0388>. See in particular art. 2: “[...] Member States shall withdraw all special or exclusive rights for the supply of telecommunications services other than voice telephony and shall take the measures necessary to ensure that any operator is entitled to supply such telecommunications services.”

<sup>25</sup> See Council of the European Communities, ‘87/499/EEC: Council Decision of 5 October 1987 Introducing a Communications Network Community Programme on Trade Electronic Data Interchange Systems (TEDIS)’, Pub. L. No. 499, EEC (1987), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31987D0499>. Its paragraph 3, point 7, compelled to “to seek solutions to legal problems that might inhibit the development of trade electronic data interchange and to see to it that restrictive telecommunications regulations cannot hamper the development of trade electronic data interchange”.

<sup>26</sup> Vittorio Frosini, ‘La Libera Circolazione dei Beni e dei Servizi Informatici nel mercato comune europeo’, *Diritto dell’informazione e dell’informatica*, no. 1 (1995): 25–26.

attempting to grasp the inherent security aspects that new technologies brought.

## II.1 The nineties: security as standardization

In this context, alongside the affirmation of “IT freedom”<sup>27</sup>, which enshrined the free transborder flow of data, as a “fuel” within the new European market, the first seeds of awareness about cybersecurity could be gathered.

The swift liberalization of communication instruments and the promotion of communication standards encouraged discussions about cybersecurity, which was becoming a universal need in the early interconnected continent.

“There [was] a strong need [...] to protect information stored on various media and/or transiting public telecommunications”, and the entire problem became even more pressing when most restrictions on transborder operations within the European Economic Community were abolished in 1992<sup>28</sup>.

Member states could no longer afford to only maintain a “cosmetic” security<sup>29</sup> and needed to pursue appropriate implementations. Therefore, if certainly “the needs for security information [were] rather uniform throughout Western Europe, [...] attitudes towards the best methods for satisfying the needs [were] even more varied”<sup>30</sup>.

Despite the variety of approaches, examples of successful coordination between member states began to emerge due to the recognition of a common necessity. If the same technologies were used in different countries, there could not be different principles to assess security. Consequently, the ultimate goal of mutual recognition at the foundation of the new European Single Market had been preceded by the development of standardized instruments for carrying out the assessment procedure. Since, in the course of only four decades, IT had started to play a vital role in almost all sectors of organised societies, the creation of a consistent methodology was only a natural response that began to fill a “security gap”. Thus, building users’ trust in technology meant primarily building trust in technology’s security, for example, identifying mandatory functionalities to be implemented to achieve a specific security objective through a security mechanism. Overall, ensuring confidence was and is the result of a complex evaluation system with objective and definite security evaluation criteria and the existence of a certification body that can confirm that the assessment has been properly conducted.

These requirements had already been discussed when assessment frameworks started to be harmonized between some member states with the aim of exploiting the benefits of mutual recognition of the same standards. After different attempts to balance security evaluation criteria, which had only been carried out at a national level<sup>31</sup>, France, Germany,

---

<sup>27</sup> The term was coined by Frosini to define an early theorizing of the right to data protection, that was born with the Convention n. 108 of the Council of Europe.

<sup>28</sup> Richard I. Polis, ‘European Needs and Attitudes Towards Information Security’, *Cryptologia* 12, no. 4 (October 1988): 235, <https://doi.org/10.1080/0161-118891862981>.

<sup>29</sup> Polis, 237.

<sup>30</sup> Polis, 234.

<sup>31</sup> For example, the Trusted Computer System Evaluation Criteria (TCSEC), commonly referred as the TCSED or as “Orange Book”, published by the US Department of Defence between late 1970s and early 1980s, can be considered the precursor of all the other frameworks in several respects. After that, many European countries developed their own IT security criteria, like the United Kingdom, where there were both a standard for governmental use (the CESG Memorandum Number 3, CESG3), and a standard for commercial security products (the so-called “Green Book”, DTIEC). At the same time, other criteria were published in Germany (ZSIEC) by the

the Netherlands, and the United Kingdom finally came to a harmonized version of security criteria in 1991, the Information Technology Security Evaluation Criteria (ITSEC). This was the first example of a cross-country and cross-sector assessment framework, founded on the accumulated experience of the participating States, which shared the best features and framed them in a consistent and structured perspective. The main achievement was an internationally compatible base for certification activities, that satisfied both companies' commercial needs and consumers' expectations, giving them an objective unit of measurement to distinguish between different products and services on the market.

Subsequently, the availability of a steady and robust framework made it possible to consolidate a common procedure, through the IT Security Evaluation Manual (ITSEM)<sup>32</sup>, which was built on ITSEC criteria to ensure a coherent set of evaluation methods. This technical document laid the foundations for the establishment of a community of certification authorities, vendors, developers, and users.

The consistent application of the rules to real cases, concerning national and international implementations, showed the flexibility of the methodological rules, but also created differences between national practices. In less than a decade, it became necessary to intervene again to maintain the initial coherence, which was slowly vanishing with continuous use.

For this reason, a Joint Interpretation Library of the ITSEC criteria was published in November 1998 to collect all the observations raised over the years by the Joint Interpretation Working Group (JIWG)<sup>33</sup>. Although the adoption of the document in each country was not mandatory, the document undoubtedly intended to supplement ITSEC criteria, aiding mutual recognition<sup>34</sup>.

---

German Information Security Agency in 1989, and in France (the so-called "Blue-White-Red-Book", SCSSI). European Commission, 'Information Technology Security Evaluation Criteria (ITSEC)', ed. Senior Officials Group - Information Systems Security (Department of Trade and Industry, 28 June 1991), 2, <https://sogis.org/documents/itsec/itsec-en.pdf>. The result of the hybridisation between these European efforts and the American TCSEC was the further spread of new endeavours, like the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), published by the Communication Security Establishment in 1993. 'Canadian Trusted Computer Product Evaluation Criteria', in *Wikipedia*, accessed 2 November 2022, [https://en.wikipedia.org/w/index.php?title=Canadian\\_Trusted\\_Computer\\_Product\\_Evaluation\\_Criteria&oldid=1103502712](https://en.wikipedia.org/w/index.php?title=Canadian_Trusted_Computer_Product_Evaluation_Criteria&oldid=1103502712).

<sup>32</sup> European Commission, 'Information Technology Security Evaluation Manual (ITSEM)', ed. Senior Officials Group - Information Systems Security, 10 September 1993, <https://sogis.org/documents/itsec/itsem-en.pdf>.

<sup>33</sup> European Commission, 'ITSEC Joint Interpretation Library (ITSEC JIL)', ed. Senior Officials Group - Information Systems Security, November 1998, <https://sogis.org/documents/itsec/ITSEC-JIL-V2-0-nov-98.pdf>.

<sup>34</sup> Soon, the ITSEC criteria would have been surpassed by the Common Criteria. Developed in the late 1990s, the Common Criteria combines elements from the European ITSEC, the United States' TCSEC (Trusted Computer System Evaluation Criteria), and Canada's CTCPEC (Canadian Trusted Computer Product Evaluation Criteria) to create a harmonized set of evaluation criteria. Not only do they provide standardized approaches to assess the security of IT products and systems, but they also facilitate the certification of security through mutual recognition of evaluation results between participating countries, such as the United States, Canada, the European Union, and many others. Just like ITSEC criteria, the Common Criteria are accompanied by a manual for coherent interpretation, the Methodology for Information Technology Security Evaluation (CEM). The Common Criteria Recognition Agreement (CCRA) ensures that products can be evaluated by competent and independent licensed laboratories, that certifications are based on the results of a limited number of certificate authorizing schemes, and, that all the certificates are recognized by all the signatory countries. For further information about common criteria see 'Common Criteria: New CC Portal', accessed 30 April 2023, <https://www.commoncriteriaportal.org/>.

While the market was independently fostering the development of technical standards, the European communities were urged to act. After several times their institutions had stressed the importance of information security, the inherent complexity of the topic justified the Commission's intervention, which implied the introduction of policies in different sectors.

The convergence between the widespread of the information market, whose value was playing a vital role in the prosecution of economic activities, and telecommunications standardization encouraged the development of a global strategy for information security with the purpose of providing users with protection against accidental or deliberate threats. The lines of action that tried to address all the unavoidable requirements for the creation of a cybersecurity framework allowed for the crystallization of the dynamic change that was ongoing at that time<sup>35</sup>.

Although information security was recognized as a pervasive and essential quality for a digital society, the awareness of this nature was only intertwined with institutions' immobilism. Clearly, the absence of an initiative to arrange the different efforts for the single market would have jeopardized its foundation. Thus, the Commission proposed to align laws to mirror the results from risk analysis, compelling the implementation of security policies, and introducing penalties for violations. Not only would this approach have promoted the debate about the technical advance of new security practices, which was spontaneously happening, but it would also have contributed to addressing it through appropriate bans and minimum requirements.

That was the first time that European institutions reasoned about security as a meta-right because it is "the inherent prerequisite for the protection of privacy, intellectual property, commercial confidentiality and national security"<sup>36</sup>. It must be stressed how this statement is even more valuable when it is correctly framed in time, considering the subsequent European policies.

The value of cybersecurity had been recognized beforehand, even if only in a proposal of the European Commission, exactly on the same year as the proposal for the so-called data protection directive (dir. 95/46/CE)<sup>37</sup>.

Each step adopted in following European policies revolved around these two fundamental components, which helped to address the early spread of technology to support a fair implementation of other fundamental rights and competition in the European market.

Whereas fundamental right protection would have been more aligned with isolation, this approach would not have allowed for the fulfilment of the idea behind the European common market. In an era characterized by swift globalization and increasing digitisation, the strategy

---

<sup>35</sup> European Commission, 'Proposal for a Council Decision in the Field of Information Security', 13 September 1990, COM/90/314FINAL, OJ C 277, 5.11.1990, p. 18–24.

<sup>36</sup> European Commission, 3.

<sup>37</sup> It is possible to refer to whereas 10 and art. 1 of dir. 95/46/CE which introduce the main purpose that is accomplished through a data protection regulation: the protection of other fundamental rights. In this perspective, it is apparent the role of privacy as a requirement to exercise another right. The same orientation is commonly shared by scholars. Refer for example to Carlo Colapietro, *Il diritto alla protezione dei dati personali in un sistema delle fonti multilivello: il Regolamento UE 2016/679 parametro di legittimità della complessiva normativa italiana sulla 'privacy'* (Napoli: Editoriale scientifica, 2018), 21–38; Simone Barbareschi and Andrea Giubilei, 'L' equilibrio tra la tutela dei dati personali e la manifestazione del pensiero', in *I dati personali nel diritto europeo*, ed. Vincenzo Cuffaro, Roberto D'Orazio, and Vincenzo Ricciuto (Torino: G. Giappichelli editore, 2019), 463.

of maintaining security through isolation has become unsuitable and unsustainable. The interconnected nature of modern societies has rendered the concept of absolute isolation impractical. In fact, the ability to access external resources and facilitate seamless communication across diverse user groups has emerged as a vital necessity, to promote the free exchange of information, drive innovation, and foster collaboration. Consequently, the crux of contemporary security paradigms must pivot from an illusory pursuit of seclusion to the implementation of robust, adaptive measures that safeguard sensitive data and systems without inhibiting essential cross-border interactions.

In circumstances where isolation is deemed unfeasible, it becomes imperative to embrace standardization to enhance information security. This approach necessitated acknowledging that “neither the technology, terminals and services nor the related standards and procedures [were] generally available to provide comparable information security [results]”<sup>38</sup>, due to their current state of development. As a result, a comprehensive and rigorous examination had to be undertaken to discern the ever-changing and dynamic information security requirements of the primary stakeholders involved. Doing so would have enabled the development and implementation of adaptable and robust security measures that cater to the diverse needs and challenges inherent within the realm of information security, ultimately paving the way for a more secure and collaborative digital landscape.

While the absence of agreed standards and specifications may have presented a major barrier to the advancement of information-based processes and services throughout the economy and society, many countries started developing criteria to assess the trustworthiness of ITs and telecommunications, as already exemplified. Notwithstanding the early attempts of development, which were proceeding at different speeds, the very close relationship between regulatory, operational, administrative, and technical aspects of information security could be easily understood. As a matter of fact, “regulations need to be reflected in standards and information security provisions need to comply in a verifiable manner to the standards and regulations”<sup>39</sup>.

This hierarchical relationship from top to bottom is the result of the necessity of more detailed specifications beyond the conventional scope of regulation. Whereas regulations’ requirements must be adopted by standards, standards’ requirements have to be concretized by practical security provisions.

An indirect consequence of this interdependence is that standards can be seen as a sort of prerequisite for the protection of fundamental rights because they became the only possible instrument to bind and guide the implementation of communication technologies and of ITs in general. By providing a harmonized framework, these standards ensure that the development and deployment of such technologies adhere to the principles of human rights and ethical considerations. Consequently, the establishment and enforcement of comprehensive standards has become an imperative aspect of both technological advancement and the preservation of societal values.

This was the only possible alternative to reconcile these two pivotal incentives, which isolation would have certainly failed to preserve both. In particular, as it has been already remarked, the main reason must be sought in the imperative purpose of competitiveness of the European economy. Notwithstanding the illusory intentions of the European lawmaker,

---

<sup>38</sup> European Commission, ‘Proposal for a Council Decision in the Field of Information Security’, 4.

<sup>39</sup> European Commission, 5.

who was building a façade displaying protection of rights, the real motive was an economic reason.

This approach can also be seen in the decision taken by the Presidency at the Corfu European Council in June 1994, which was supported by a White Paper commissioned by the European Commission from various expert groups<sup>40</sup> set up to clarify the consequences that the wave of digitalisation would have on European society. The chapter about the global information society, was also known as “Bangemann’s report”<sup>41</sup>, after the name of the group of experts who worked on this subject. They underlined how “all revolutions generate uncertainty, discontinuity and opportunity”<sup>42</sup>, and immediately foresaw the huge impact on human intelligence, hence on the way of working and living. Apart from the need of fostering a generalised access to the new technology, “preparing Europeans for the advent of information society”, the main question was “whether [that would be] a strategic creation for the whole Union, or a more fragmented and much less effective amalgama of individual initiatives by Member States”<sup>43</sup>. After having recognized the considerable benefits, the report advocates an action plan which could stimulate markets. That vision deemed private investment as the driving force of the digital revolution, and monopolistic, anticompetitive environments as the real roadblocks<sup>44</sup>. There was an evident need to stimulate competition to such an extent that even interventions for a uniform regulation of rights were merely mentioned as instruments for a better functioning of the market, a mere way of “completing the agenda”<sup>45</sup>.

While it may be challenging to characterize the driving force behind this endeavour as purely altruistic or as a steadfast defender of liberties, it is crucial to acknowledge that these seemingly less noble ideals have, in fact, provided the necessary impetus for subsequent efforts in advancing technological standardization. This undertaking demanded a comprehensive examination of the technology landscape, encompassing the development and execution of strategic plans, the identification and employment of cutting-edge technologies, as well as the ensuing integration and verification of these components.

Furthermore, the establishment and early development of security technology necessitated a cohesive and comprehensive framework, which included a series of supplementary measures to ensure the generation, preservation, and consistent application of standards. This framework also facilitated the validation and certification of information technology and telecommunication products, thus promoting a more reliable and interconnected global infrastructure.

The establishment of a robust and dependable framework is undeniably a consequence of intricate coordination efforts, which serve as the bedrock for assigning roles within the system. Specifically, the implementation, validation, and subsequent mutual recognition of

---

<sup>40</sup> European Commission, ‘Growth, Competitiveness and Employment - White Paper Follow-Up’ (Luxembourg, 1994).

<sup>41</sup> Bangemann group, ‘Europe and the Global Information Society - Recommendations of the High-Level Group on the Information Society to the Corfu European Council (Bangemann Group)’, in *Growth, Competitiveness and Employment White Paper Follow-Up* (Luxembourg, 1994), [http://aei.pitt.edu/1199/1/info\\_society\\_bangeman\\_report.pdf](http://aei.pitt.edu/1199/1/info_society_bangeman_report.pdf).

<sup>42</sup> Bangemann group, 10.

<sup>43</sup> Bangemann group, 11–12.

<sup>44</sup> Bangemann group, 13.

<sup>45</sup> Bangemann group, 21–24.

standards serve as the principal requirements for the effective functioning of such a structure. In the word of the Bangemann's report, if "the European information society is emerging from many different angles" and "European infrastructure is evolving [...], assembling the various pieces of this complex system to meet the challenge of interoperability would be impossible without clear conventions. Standards are such conventions"<sup>46</sup>.

Although the organization at a European level predominantly operates through informal networks, and mutual recognition of verification and certification remains confined to closed groups, the ultimate goal was to achieve a well-defined and consensual distribution of responsibilities among the various actors at the Community level. This harmonization of roles is deemed essential as a prerequisite for fostering mutual recognition and facilitating greater cooperation and efficiency within the system.

The culmination of the concerted efforts delineated was ultimately solidified by a resolution from the Council of the European Communities<sup>47</sup>, which effectively initiated the action plan as outlined in the European Commission's proposal. In addition to this, the Council took the crucial step of establishing a Senior Officials Group (SOG-IS) with the primary function of assessing the progress made and offering guidance to the Commission on the necessary measures to be implemented within the realm of information security.

Concurrently, within the same year, the Commission presented a supplementary proposal aimed at steering the independent advancements generated by the market concerning security evaluation criteria for information technology<sup>48</sup>. Garnering the endorsement of both the Economic and Social Committee and the European Parliament<sup>49</sup>, the Council subsequently intervened to reinforce the application of ITSEC, with the objective of achieving enhanced harmonization at the European level and facilitating the improved mutual recognition of security evaluation certificates<sup>50</sup>.

Overall, that was the "Europe's way to the information society"<sup>51</sup>. In an early interconnected world, the European Union accelerated its efforts towards the creation of a unique common market. Since the establishment of the European Community with the Maastricht treaty in 1992, Europe has sought to safeguard the benefits of the Community and avoid "risks [...] that handling these matters nationally or the duplication by the Member States of Community measures would entail", as correctly stressed by the European

---

<sup>46</sup> Bangemann group, 18.

<sup>47</sup> Council of the European Union, 'In the Field of Security of Information Systems', 31 March 1992, 92/242/EEC, <https://op.europa.eu/en/publication-detail/-/publication/2b0db115-a244-464f-a4ab-2e28d1a5a9ab>.

<sup>48</sup> European Commission, 'Proposal for a COUNCIL RECOMMENDATION ON COMMON Information Technology Security Evaluation Criteria', 10 September 1992, COM/92/298FINAL, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:51992PC0298>.

<sup>49</sup> European Commission, 'Amended Proposal for a Council Recommendation on Common Information Technology Security Evaluation Criteria', 9 February 1994, COM/94/37FINAL, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:51994PC0037>.

<sup>50</sup> Council of the European Union, 'Council Recommendation of 7 April 1995 on Common Information Technology Security Evaluation Criteria', 7 April 1995, 95/144/EC, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995H0144>.

<sup>51</sup> European Commission, 'Communication from the Commission to the Council and the European Parliament and to the Economic and Social Committee and the Committee of Regions - Europe's Way to the Information Society. An Action Plan', 19 July 1994, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A51994DC0347&qid=1682951576431>.



Parliament<sup>52</sup>.

European policy can therefore be broken down into different levels of intervention, reflecting both the growth in demand and the growth in the scope of digital services.<sup>53</sup>

The first were technical interventions to ensure interconnection, interoperability and spectrum allocation. These were the foundations of the telecommunications system after the 1987 Green Paper<sup>54</sup>, which paved the way for the essential standardisation required by the technology<sup>55</sup>.

While this first layer allows the technology to function properly, the second layer concerns its inherent economic dimension. The focus is not on functionality, but on ensuring an appropriate regulatory framework for electronic communications, whose minimum requirements are market access and competition<sup>56</sup>. Therefore, the aim was to promote the creation of a digital marketplace by advocating, particularly, the liberalisation of telecommunications instruments.

Despite the efforts, these essential conditions were still lingering with many other distortions and sectoral obstacles<sup>57</sup>, which had to be dismantled, as Mario Monti remembered in 1997 in his speech as European Commissioner<sup>58</sup>. Due to the number of interests and stakeholders involved, the task was complex and required a variety of legal interventions, which ideally represent the last layer.

Although the economic perspective was preeminent, many of these regulations certainly refer to the protection of some individual rights, considering a public role inside the market.

Besides the introduction of the first privacy directives<sup>59</sup> or the database directive, further

---

<sup>52</sup> European Commission, 'Resolution on the Recommendation to the European Council: ' Europe and the Global Information Society' and the Communication from the Commission to the Council and the European Parliament and to the Economic and Social Committee and the Committee of the Regions: ' Europe' s Way to the Information Society: An Action Plan'', 28 November 1994, COM(94)0347, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:51996IP0244>.

<sup>53</sup> European Commission, 'Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - Globalisation and the Information Society - The Need for Strengthened International Coordination', 4 February 1998, 4, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A51998DC0050&qid=1683984191563>.

<sup>54</sup> European Commission, 'Towards a Dynamic European Economy, Green Paper on the Development of the Common Market for Telecommunications Services and Equipment'.

<sup>55</sup> Two examples of famous standards, which are part our daily life are the GSM (Global System for Mobile Communication) and DNS (Domain Name System).

<sup>56</sup> European Commission, 'Green Paper on the Convergence of the Telecommunications, Media and Information Technology Sectors, and the Implications for Regulation - Towards an Information Society Approach', 3 December 1997, 20–27, COM/97/0623 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A51997DC0623&qid=1684076807163>.

<sup>57</sup> European Commission, 'Communication from the Commission to the European Parliament and the Council - Draft Action Plan for the Single Market', 6 May 1997, 9–11, COM/97/0184 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A51997DC0184&qid=1684500102416>.

<sup>58</sup> Monti Mario, 'Speech by Mario MONTI - European Commissioner for the Single Market - Electronic Commerce in Europe - Creating a Favourable Environment for Electronic Commerce', 8 July 1997, SPEECH/97/157, [https://ec.europa.eu/commission/presscorner/detail/en/SPEECH\\_97\\_157](https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_97_157).

<sup>59</sup> A more specific directive about privacy in telecommunications sector was approved few years later. See European Parliament and Council of the European Union, 'Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector', 024 OJ L § (1997), <https://eur-lex.europa.eu/legal->

steps were taken in the fields of electronic payments<sup>60</sup> and digital signatures<sup>61</sup>.

All these regulations were needed to set boundaries to the new uses made possible by digitisation and contributed to set some minimum-security requirements. Even if the trust in the digital market was the main reason, it should not go unnoticed how the multiple interventions of the European legislator converged in contributing to the protection of rights. In this context, security stood out as an undeniable building block, albeit not consolidated in a specific piece of legislation, but its nuances must be grasped through a careful examination of other legislation.

## II.2 The new millennium: security as a reaction to threats

Keeping in mind the approach to security as an instrument for the bigger goal of European integration, which has already been described for the nineties, the main politics for the subsequent decade must be analysed<sup>62</sup>.

### II.2.1 eEurope 2002 strategy (1999-2002)

The very lack of a clear set of rules must be acknowledged, as the European lawmaker was focused on the ultimate aim of fostering better connectivity around the continent because “Europe [was] not fully exploiting this potential as it is not moving fast enough into the digital age”<sup>63</sup>. In this context, security was perceived as an important competition boost both as a good in the market and as an access key to the market itself.

The first conception was the result of the attempts to develop encryption technologies, which are a requirement for electronic transactions and, in general, for electronic banking. On the other hand, the second idea was a natural extension of this development since encryption is the foundation for any form of secure access or secure communication. That said, the beginning of a self-feeding phenomenon could be glimpsed. For this reason, there was high attention for the definition of appropriate standards in this field, because “if Europe [could] lead the development of these technologies, huge markets [would] open up”<sup>64</sup>.

On the following year, the Lisbon Council consolidated the objectives set by European Commission, setting the strategic goal “to become the most competitive and dynamic knowledge-based economy in the world capable of sustainable economic growth with more and better jobs and greater social cohesion”<sup>65</sup>. This meant to focus on the review of the

---

content/EN/TXT/?uri=CELEX:31997L0066.

<sup>60</sup> European Parliament and Council of the European Communities, ‘Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the Taking up, Pursuit of and Prudential Supervision of the Business of Electronic Money Institutions’, 275 OJ L § (2000), <http://data.europa.eu/eli/dir/2000/46/oj/eng>.

<sup>61</sup> European Parliament and Council of the European Union, ‘Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures’, Pub. L. No. 93, EC (1999), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0093>.

<sup>62</sup> The subdivision of the next paragraphs follows the three steps of the eEurope strategy proposed by European Commission, as recalled by Centre for Europe, University of Warsaw, Poland and Grabowska, ‘Legal, Political and Organizational Aspects of Cybersecurity in the European Union’, 110.

<sup>63</sup> European Commission, ‘eEurope - An Information Society for All - Communication on a Commission Initiative for the Special European Council of Lisbon, 23 and 24 March 2000’, 8 December 1999, 1, COM/99/0687 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:51999DC0687>.

<sup>64</sup> European Commission, 11.

<sup>65</sup> Council of the European Union, ‘Lisbon European Council 23-24.03.2000: Conclusions of the Presidency’, 23 March 2000, [https://www.europarl.europa.eu/summits/lis1\\_en.htm?textMode=on](https://www.europarl.europa.eu/summits/lis1_en.htm?textMode=on).

regulatory framework for telecommunication, the so-called “telecom package”<sup>66</sup>, and on that “legal layer” of interventions<sup>67</sup>, as it has just been referred in the previous paragraph, which were supposed to advocate the effects of connectivity, supporting users trust towards the digital market.

These ambitious cornerstones were asking for the definition of a precise action plan<sup>68</sup>, which could allow for a step-by-step measurement of the advancements. Therefore, European Commission, entrusted with the definition of the plan, adopted a shared benchmarking system to interpret the data from all the European initiatives at different levels.

The agenda had three objectives: better connectivity, proper training for digital skills, and incentives to the Internet’s use. There was a strong continuity with the topics of infrastructures and of the disposal of the obstacles to their use, which were deemed as the most effective approaches for their capability to horizontally encompass different fields.

Considering only the milestones, apart from frequencies and competition issues, telecom infrastructures were being developed urging the adoption of secure standards<sup>69</sup>. In addition, connectivity was also recognized as an essential tool for safety, unlocking new possibilities for protecting citizens in need<sup>70</sup>. The implementation of innovative services for e-health and e-government was being advocated, and security of access was the prime requirement for their success. In this phase, the main incentives to the use of the Internet were represented by the digitisation of more and more public services, at least on paper. In fact, the focus of the legal layer's interventions was mainly on promoting e-commerce, rather than on a rights perspective.

---

<sup>66</sup> The 2002 Telecom Package by the European Union aimed to modernize and liberalize the telecommunications market in Europe. The main regulatory interventions included: a) Establishment of a common regulatory framework for electronic communications services; b) Introduction of competition rules to prevent anti-competitive market behaviour; c) Promoting universal service obligations to ensure essential communications services for all users; d) Requiring transparent and non-discriminatory access to networks and services; e) Strengthening the powers of national regulators to enforce compliance with the rules. These measures were intended to create a level playing field for market players, enhance consumer protection, and stimulate innovation in the industry. For more further information about the steps of harmonization of European telecommunications see Fabrizio Dalle Nogare, ‘Le comunicazioni elettroniche: evoluzione del quadro istituzionale e prospettive’, in *Regolazione e mercato delle comunicazioni elettroniche: la storia, la governance delle regole e il nuovo Codice europeo* (Torino: G. Giappichelli Editore, 2019), 22–34.

<sup>67</sup> A progress report submitted to the Lisbon Council underlined in particular the advancements on telecom liberalisation and on e-commerce. There were only some coordination attempts about the other points of the agenda. See European Commission, ‘eEurope - An Information Society for All - Progress Report for the Special European Council on Employment, Economic Reforms and Social Cohesion towards a Europe Based on Innovation and Knowledge Lisbon, 23 and 24 March 2000’, 8 March 2000, 9–11, COM/2000/0130 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52000DC0130&qid=1685639413472>.

<sup>68</sup> European Commission, ‘eEurope 2002 - An Information Society for All - Draft Action Plan Prepared by the European Commission for the European Council in Feira - 19-20 June 2000’, 24 May 2000, COM (2000) 330 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52000DC0330>.

<sup>69</sup> The reference is to IPv6 or Internet Protocol version 6, a network addressing protocol that provides a significantly larger address space than its predecessor, IPv4. It uses 128-bit addresses and supports a variety of features, including flow labelling, quality of service (QoS), and security enhancements. IPv6 was developed to address the growing shortage of IPv4 addresses and to improve the efficiency, scalability, and flexibility of the internet. See European Commission, 8.

<sup>70</sup> The reference was to the ability to locate the position of callers to the European emergency number 112. See European Commission, 28. This feature is a current obligation.

But security was beginning to find another fundamental way of expressing itself, the activities to counter cybercrime, which for the first time became part of a general European policy<sup>71</sup>.

In the nineties, a preliminary attention to the topic could be identified in those discussions about fighting illegal contents. European Commission submitted studies about the phenomenon, stressing its relationship with several areas of law<sup>72</sup>. Online contents were causing a problem of balance between the protection of rights and the principle of the free flow of information. On the one hand, what is illegal offline remained illegal online, so the issue was the enforcement of the existing laws by member states. "The Internet does not exist in a legal vacuum, since all those involved [...] are subject to the respective laws of the Member States"<sup>73</sup>. On the other hand, the adoption of national restrictive rules against service providers could have some drawbacks. In this sense, "the presence of illegal and harmful content on the Internet [had] direct repercussions on the workings of the Internal Market"<sup>74</sup>.

After having analysed the functioning behind the Internet, European institutions underlined what main consequences for the current traditional regulation needed to be immediately addressed. The first emerging limitation concerned law enforcement, due to the international scope of criminal activities, which had become easier with the spread of new IT technologies. Furthermore, the inherent dematerialization of contents prevents their definitive deletion since everything can be effortlessly copied into other jurisdictions. The only solution to this technical problem was to establish an improved coordination mechanism, exploiting Europol framework and setting minimum recognized standards for illegal contents.

This brings to another natural consequence, concerning one of the first debates about the role of internet and service providers, topic which have been developed by scholars since recent times. Because of the nature of networking, many intermediaries are involved in an electronic connection. "It is therefore essential to identify accurately the chain of responsibilities in order to place the liability for illegal content on those who create it"<sup>75</sup>. Today, as in the past, it is crucial to define the procedures for removing or blocking access to online contents.

That communication of the European commission was coordinated with another one specifically focused on the protection of minors from illegal or harmful contents, which was able to depict the ongoing change. "The transition from a broadcast world to an environment where conventional television will exist alongside on-line services and indeed hybrid products creates a host of opportunities. The full potential of such developments will depend on society as a whole striking the right balance between freedom of speech and public interest

---

<sup>71</sup> George Christou, 'The European Union and Cybercrime', in *Cybersecurity in the European Union* (London: Palgrave Macmillan UK, 2016), 90, [https://doi.org/10.1057/9781137400529\\_5](https://doi.org/10.1057/9781137400529_5). The author remarks the innovative relationship between "the salience of addressing issues of network security and combating cybercrime".

<sup>72</sup> European Commission, 'Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - Illegal and Harmful Content on the Internet', 16 October 1996, COM/96/0487 FINAL, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A51996DC0487&qid=1684518587373>.

<sup>73</sup> European Commission, 10.

<sup>74</sup> European Commission, 4.

<sup>75</sup> European Commission, 13.

considerations, between policies designed to foster the emergence of new services and the need to ensure that the opportunities they create are not abused by the few at the expense of the many”<sup>76</sup>. Those consideration was consolidated in a subsequent recommendation of the Council<sup>77</sup>.

Overall, the focus in the nineties was on the fight against illegal content rather than crime per se. The only attempt in this direction can be found in a study commissioned by the European Commission, the so-called COMCRIME study<sup>78</sup>.

For a more coherent approach to cybercrime by Europe, we must wait until the Action Plan of European Commission to the Feira Summit of the European Council<sup>79</sup>, which, in fact, was followed by another specific communication on the topic<sup>80</sup>. As digitisation could open new possibilities for European citizens, the same instruments could also be abused for perpetrating and facilitating various criminal activities.

European institutions were making a breakthrough in understanding that the “classical security approach called for strict organisational, geographic, and structural compartmentalisation of information according to sensitivity and category. This is no longer really feasible in this digital world since information processing is distributed, services follow mobile users and interoperability of systems is a prerequisite”<sup>81</sup>.

If digital infrastructure became a critical part of European economy, it had to be reliable, assuring safety both of communications and data.

Although the efforts in the field were only at an embryonic step, it is of utmost interest to remark that classic dichotomy about tackling cybercrime, which was going to be consolidated in further regulations.

On the one hand there were all problems related to criminal law harmonization to address both substantive and procedural law issues. The first needed an intervention to ensure a minimum level of protection, starting from the international standard embodied by Council of Europe’s Convention on cybercrime. Thus, the aim of the European Union was to go further, deepening its level of integration. The latter necessitated to empower law enforcement agencies to investigate and request cooperation from other European countries. These needs are commonly related to invasive uses of technologies like, for example, interception of communications, retention of communications’ metadata, so they have to

---

<sup>76</sup> European Commission, ‘Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services’, 16 October 1996, 4, COM/96/0483 FINAL, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A51996DC0483&qid=1684518698752>.

<sup>77</sup> Council of the European Communities, ‘98/560/EC: Council Recommendation of 24 September 1998 on the Development of the Competitiveness of the European Audiovisual and Information Services Industry by Promoting National Frameworks Aimed at Achieving a Comparable and Effective Level of Protection of Minors and Human Dignity’, *OJ L*, 24 September 1998, <http://data.europa.eu/eli/reco/1998/560/oj/eng>.

<sup>78</sup> Ulrich Sieber, ‘Legal Aspects of Computer-Related Crime in the Information Society (COMCRIME Study)’ (University of Würzburg, April 1998).

<sup>79</sup> European Commission, ‘eEurope 2002 - An Information Society for All - Draft Action Plan Prepared by the European Commission for the European Council in Feira - 19-20 June 2000’.

<sup>80</sup> European Commission, ‘COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime’, 26 January 2001, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52000DC0890>.

<sup>81</sup> European Commission, 6.

find the right balance with fundamental rights.

While the first order of problems concerned criminal law, as one could expect, the second one was more subtle, but it was growing in importance. The realisation that cybercrime is the product of information infrastructures' insecurity is being referred to. Information society was replacing old generation networks with Internet, whose security have to be handled accordingly.

Although the Internet's core is simple because is only dedicated to the task of transmitting data, there are other several security aspects. For example, the integration of user environment in the network requires implementation of security techniques, since it becomes a key part of the information infrastructure. At the same time, the spread of access called for an increasing variety of authentication mechanism to grade different level of permissions. Therefore, encryption and electronic signatures started to be an essential part of the Internet daily use.

The essential simplicity behind the mechanisms of the network of networks was exactly the main issue, which elicited a race against time to fix that initial insecurity by design approach. The only way was to implement new layers, adding complexity afterwards. The development of security software and the implementation of authentication systems have already been mentioned, but the construction of entirely new infrastructures was involved. One of the most important ones is the public-key infrastructures (PKI)<sup>82</sup>, which is the bedrock for the trust in the ownership of digital services identity.

While intervening *ex post* was the first solution, it could not be a viable and definite way out. This was clear to the European Commission which underlined how "it [was] important also that any future conceptual framework for security be an integral part of the overall architecture, addressing threats and vulnerabilities from the outset of the design process". That way of thinking security was apparently in contrasts "with traditional add-on approaches, which have necessarily attempted to plug the holes exploited by an increasingly sophisticated criminal community"<sup>83</sup>.

---

<sup>82</sup> Public Key Infrastructure (PKI) is a security architecture that provides a framework for managing digital certificates and public key encryption. It enables secure and authenticated communication over an insecure medium such as the Internet. In a PKI, a trusted third party (called a Certificate Authority - CA) issues digital certificates that bind the identity of an entity (such as a person or organisation) to a public key. These certificates are digitally signed by the CA and can be used to verify the identity of the owner of the certificate when communicating over a network. To send an encrypted message securely in a PKI, the sender encrypts the message using the recipient's public key, which is available in the recipient's digital certificate. The recipient can then decrypt the message using their private key, which is securely stored at their end. PKI also provides a mechanism for revoking and updating certificates. Revocation is necessary when a certificate is compromised, the associated private key is lost, or the identity of the certificate holder is no longer valid. To prevent compromised certificates from being used, CAs maintain a list of revoked or invalid certificates known as a Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP). PKI is widely used in applications such as secure email, e-commerce and government services. For example, online banking websites often use PKI to authenticate the user's identity and establish secure communication between the bank's server and the user's web browser over the Internet. In summary, PKI is a security framework that uses digital certificates and encryption to provide secure communication over an insecure network such as the Internet. It relies on a CA to issue and manage digital certificates and uses public key encryption to enable secure communication between entities. For further information see Jingwei Huang and David M. Nicol, 'An Anatomy of Trust in Public Key Infrastructure', *International Journal of Critical Infrastructures* 13, no. 2–3 (2017): 238–58, <https://doi.org/10.1504/IJCIS.2017.088234>.

<sup>83</sup> European Commission, 'COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN

Although the vision behind the intention was already modern in its conception, the results towards its pursuit were proceeding in small steps. The new digital economy was expecting a faster legislative intervention which was able to link together benchmarks results and best practices to policy implementation. Despite the strong political interest in the exploitation of the new possibilities, there were long delays. The efforts of the members states needed to be more effectively linked<sup>84</sup>. The first result from the monitoring of the plan clearly stated that “that the full potential of these digital technologies for efficiency gains is not yet being exploited”<sup>85</sup>, but previous attentions to telecom infrastructures is confirmed.

The European lawmaker had already approved both an e-commerce and an electronic signatures directive, which were being implemented by Member States, while the telecom package was nearing its approval.

At the same time, that part of interventions that were more focused on security was remarking the necessity of the double approach already recalled to face cybercrime. Therefore, criminal activities had to be banned and appropriately punished, but also discouraged setting some minimum common security requirement for authentication mechanisms and introducing a first cooperation between national CERTs (Computer Emergency Response Teams)<sup>86</sup>.

At the Stockholm Council, the EU Council advocated a more incisive approach to security, calling for the full cooperation of the Commission<sup>87</sup>. This paved the way for a first proposal for a European Policy Approach which tried to resume the main actions about the topic, even if “finding an adequate policy response [was] becoming an increasingly complex task”. Despite this, “a substantial body of legislation as part of the telecommunications framework and data protection law have been put in place both at national and EU level”<sup>88</sup>. In an attempt to bring order to a fragmented and heterogeneous set of interventions, the Commission had distinguished three areas of interest, united by the effort to ensure security. As a confirmation of what has already been said before, security is decomposed into telecommunication and data protection policies, network and information security policies, and cybercrime policies. While the protection of privacy has been a key policy objective from the beginning due to its explicit recognition by the European Treaties and the Charter of Fundamental Rights of the

---

PARLIAMENT, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime’, 11.

<sup>84</sup> European Commission, ‘Communication from the Commission to the Council and European Parliament - The eEurope 2002 Update Prepared by the European Commission for the European Council in Nice, 7th and 8th December 2000’, 29 November 2000, 6, COM/2000/0783 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52000DC0783&qid=1685684370134>.

<sup>85</sup> European Commission, ‘Communication from the Commission to the Council and the European Parliament - eEurope 2002: Impact and Priorities A Communication to the Spring European Council in Stockholm, 23-24 March 2001’, 13 March 2001, 10, COM/2001/0140 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52001DC0140>.

<sup>86</sup> European Commission, 15–16.

<sup>87</sup> Council of the European Union, ‘Presidency Conclusions - European Council Stockholm’, 26 March 2001, 12, [http://aei.pitt.edu/43341/1/Stockholm\\_2001.pdf](http://aei.pitt.edu/43341/1/Stockholm_2001.pdf).

<sup>88</sup> European Commission, ‘Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach’, 6 June 2001, 2, COM/2001/0298 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52001DC0298>.

European Union, the other policies were condensing a more recent debate. The two directions were respectively tackling digital infrastructure insecurity and the new type of offence<sup>89</sup>.

The extent of these fields is a portrayal of the horizontal effort needed to enforce security in the era of convergence and globalization. This allows to contextualize the request of the EU Council, which was urging actions by Member States for a prompt implementation of eEurope 2002 plan. “The complex nature of network and information security means that in developing policy measures in this field, public authorities must take into account a range of political, economic, organisational and technical aspects, and be aware of the decentralised and global character of communication networks”<sup>90</sup>. If during the nineties the coordination was limited to the European Union, the new dimension of technology compelled a broader course of action<sup>91</sup>.

Although the concept of security had surely changed, as well as its importance, the objectives set by the Lisbon strategy were still far to be achieved<sup>92</sup>. Some advancement reports of eEurope 2002, in fact, described “sharp contrasts and a mixed picture as regards the arrival of the information society in EU Member States”<sup>93</sup>. E-commerce was facing difficulties and was growing much slower than expected, while many countries were lacking of proper Internet penetration in comparison to leading EU Member States. Nevertheless, the result of this benchmarking has to be properly placed in context, since the assessments concerned only a first step of the general plan, and progresses cannot be measured over a short time.

Overall, seeing the achievements in a long-term perspective allows to conclude that eEurope 2002 attained its main objectives, fostering the development of the Internet, through the creation of a legal framework in e-commerce and the ongoing development of proper rules to further accompany the evolution of telecoms. As a result, many other digital services were born, also bringing administrations online with some basic e-governments services<sup>94</sup>.

---

<sup>89</sup> European Commission, 24–26.

<sup>90</sup> Council of the European Union, ‘Council Resolution of 28 January 2002 on a Common Approach and Specific Actions in the Area of Network and Information Security’, 28 January 2002, 2, OJ C 43, 16.2.2002, p. 2–4, [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002G0216\(02\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002G0216(02)).

<sup>91</sup> Common criteria (ISO-15408) are an example of this extension. While the first European efforts had brought to ITSEC criteria, the global interconnection among networks soon required another shared standard. Common Criteria (CC) is based on ITSEC (Information Technology Security Evaluation Criteria). The ITSEC criteria were developed independently by each country, making it difficult to harmonize evaluations for international security cooperation. In response to this issue, the Common Criteria was created in the mid-1990s as a collaborative international standard for evaluation criteria, which harmonized the security evaluation requirements of multiple nations. The CC also addressed some of the limitations of the ITSEC criteria, specifically in regard to providing clear and unambiguous guidance for evaluators and thereby contributing to an enhanced level of quality assurance on security products. For further information see ‘Common Criteria: New CC Portal’.

<sup>92</sup> European Commission, ‘Communication from the Commission to the Spring European Council in Barcelona - The Lisbon Strategy - Making Change Happen’, 15 January 2002, 7, COM/2002/0014 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52002DC0014>.

<sup>93</sup> European Commission, ‘Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - eEurope Benchmarking Report - eEurope 2002’, 5 February 2002, 17, COM/2002/0062 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52002DC0062&qid=1685639413472>.

<sup>94</sup> European Commission, ‘Communication from the Commission to the Council, the European Parliament,



### II.2.2 eEurope 2005 strategy (2002-2005)

In the meanwhile, the European Commission already started working on the next step of the plan to be presented to the EU Council. The following strategy, the so-called eEurope 2005 strategy, focused on less but pivotal points and kept about the same span of time of the previous one, as suggested by the Council in its Barcellona meeting. The idea was to concentrate efforts on less, but strategic issues, which were required to consent further policy development: “the widespread availability and use of broadband networks throughout the Union by 2005 and the development of Internet protocol IPv6 .... and the security of networks and information, eGovernment, eLearning, eHealth and eBusiness”<sup>95</sup>.

On the one hand there was the lingering topic of enhancing connectivity, an issue that remained central from the outset of the Lisbon strategy. On the other hand, another neuralgic theme was that of security, which is found both as the protection of the network infrastructure and as the more general protection and reliability of a range of services.

The relationship between infrastructure and service is exactly the point where the development of the subsequent steps took place. If eEurope 2002 had been mainly focused on extending Internet connectivity, that was the right moment for starting to harvest the fruits of the Internet’s penetration, translating them into new economic activities.

Since “by the end of 2002 there was little evidence to show that the success in getting Europe online had translated into new jobs and services”<sup>96</sup>, this explains the high attention on these aspects. “This is what users [were] interested in, and this [was] where eEurope 2005 start[ed] from. The objective of this Action Plan [was] to stimulate secure services, applications and content based on a widely available broadband infrastructure.”<sup>97</sup>

The idea was to foster a virtuous circle between the introduction of new services and the capability of attracting investments, while keeping the same benchmarking methodology to dynamically check the results and reviewing actions, notwithstanding the flexibility which characterize the plan. In fact, benchmarking was again one of the four essential lines at the base of the strategy.

The other lines essentially concerned policy measures to adapt legislation and their effective implementation. Not only introducing new rules was necessary, but there was also an effort towards their synergic coordination thanks to the work of an appointed steering committee.

---

the Economic and Social Committee and the Committee of the Regions - eEurope 2002 Final Report’, 11 February 2003, 18–19, COM/2003/0066 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52003DC0066&qid=1685639413472>.

<sup>95</sup> European Commission, ‘Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - eEurope 2005: An Information Society for All - An Action Plan to Be Presented in View of the Sevilla European Council, 21/22 June 2002’, 28 May 2002, 6, COM/2002/0263 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52002DC0263>.

<sup>96</sup> European Commission, ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Final Evaluation of the eEurope 2005 Action Plan and of the Multiannual Programme (2003-2006) for the Monitoring of eEurope 2005 Action Plan, Dissemination of Good Practices and the Improvement of Network and Information Security (Modinis)’, 21 August 2009, 3, COM/2009/0432 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52009DC0432&qid=1685698009806>.

<sup>97</sup> European Commission, ‘Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - eEurope 2005’, 8.

In this way, there was both an overview and a focus on the execution phase of each individual measure. Every good practice was identified and selected to verify the feasibility of the expansion of its scope of applicability, producing guidelines to be disseminated among the other Member States.

Coming to the policies, a vast array of interventions to digitize the different aspects of the relationship between the State and the citizens was set to start. As has already been recalled, one of the main issue was the introduction of e-government to steer the development of public decisions, incorporating inputs from interested actors. Despite the advancement in the implementation of smart-cards and electronic signatures, many digital public services had only limited interactivity. Undoubtedly, the affirmation of a digital state was at an embryonic step, but the objective was to enhance and coordinate all the initiatives at different levels<sup>98</sup>.

The same can be said about the digitisation of the health sector, a field that was becoming more and more information intensive. New technologies would have provided for the analysis of information, reducing administrative costs. The eEurope strategy was finally the occasion to combine the results of more than years of previous and scattered research, helping to deliver visible outcomes<sup>99</sup>.

Disregarding other aspects, which would not be beneficial to this description, it must to be stressed how security remained as an essential pillar for both of the topics, an inherent requirement that found important space within the overall European plan. While a number of initiatives had been already completed as a part of eEurope 2002, that was the moment to exploit that provided bedrock for a secure infrastructure to foster the introduction of secure and trustworthy services.

The work on the roll out of the European smart card infrastructure is mentioned, but only as a starting point for other coming actions, like the establishment of secure communications between public administrations. At the same time, technical advancements in security had to be complemented with the dissemination of good practices and awareness for a culture of security. Overall, those objectives were not something new because they can be recognized both in previous policies about infrastructure and digital skills.

The real turning point was the proposal for the creation of a cyber security task force (CSTF) to be the core for European cooperation on network and information security. On the paper, the new structure would have improved the sharing of good practices to tackle incidents, facilitating transborder collaboration.

It also deserves to be emphasised how the European Commission correctly grasped the cross-pillar dimension of cybersecurity, a character that would have been appropriately addressed to effectively implement the task force<sup>100</sup>. Therefore, even if the suggestion had already been welcomed by EU Council<sup>101</sup>, more clarity was needed about how to execute it.

The presentation of the eEurope 2005 plan was immediately followed by another proposal of the Commission to guarantee the appropriate support in terms of monitoring and funds to the realization of the project. A multi-annual program would have supported the advancements towards the Lisbon's goals, helping to portray the cross-sectorial effects of

---

<sup>98</sup> European Commission, 9–11.

<sup>99</sup> European Commission, 12–13.

<sup>100</sup> European Commission, 15–16.

<sup>101</sup> Council of the European Union, 'Council Resolution of 28 January 2002 on a Common Approach and Specific Actions in the Area of Network and Information Security', 3.

information society in different areas of activities<sup>102</sup>.

After having reached a common position with the EU Council, which only amended some minor aspects<sup>103</sup>, the decision n. 2256/2003/EC<sup>104</sup> consolidated the framework, whose general principles of functioning were similar to eEurope. Benchmarking and dissemination of good practices can be deemed as an irreplaceable piece not only for European policies but also for incorporating security as a structural value.

“Network and information security became a prerequisite for further progress of a secure business environment”. Therefore, security policy measures had to become part of the European approach to support Member States with data collection and dissemination of good practices<sup>105</sup>.

Notwithstanding the good intentions, the establishment of a stable European structure was actually the catalyst that was lacking in the overall organization. Faced with the rise of cybercrime, the European Commission had already stressed the importance of setting up national intervention groups<sup>106</sup>. Even if many countries had not immediately complied, that was only a local intervention.

Following a further request from the European Parliament for legislative action<sup>107</sup> to address the problem, the European Commission started working on a proposal to establish a European Agency for Network and Information Security<sup>108</sup>.

The working behind it had emerged also in the amendments of the MODINIS program presented by the EU Council, which cancelled the mention to a “cyber-security task force”, substituting it with a more generic reference to a “future structure” dedicated to the topic<sup>109</sup>.

---

<sup>102</sup> European Commission, ‘Proposal for a Council Decision Adopting a Multi-Annual Programme (2003-2005) for the Monitoring of eEurope, Dissemination of Good Practices and the Improvement of Network and Information Security (MODINIS)’, 26 November 2002, 5, COM/2002/0425 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52002PC0425>.

<sup>103</sup> Council of the European Union, ‘Common Position (EC) No 39/2003 of 26 May 2003 Adopted by the Council, Acting in Accordance with the Procedure Referred to in Article 251 of the Treaty Establishing the European Community, with a View to Adopting a Decision of the European Parliament and of the Council Adopting a Multiannual Programme (2003 to 2005) for the Monitoring of the eEurope 2005 Action Plan, Dissemination of Good Practices and the Improvement of Network and Information Security (MODINIS)’, 26 May 2003, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52003AG0039>.

<sup>104</sup> Council of the European Union and European Parliament, ‘Decision No 2256/2003/EC of the European Parliament and of the Council of 17 November 2003 Adopting a Multiannual Programme (2003-2005) for the Monitoring of the eEurope 2005 Action Plan, Dissemination of Good Practices and the Improvement of Network and Information Security (MODINIS)’, 17 November 2003, OJ L 336, 23.12.2003, p. 1–5, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003D2256>.

<sup>105</sup> European Commission, ‘OJ C 291E’, 26.11.2002, p. 243–249’, 5.

<sup>106</sup> Council of the European Union, ‘Council Recommendation of 25 June 2001 on Contact Points Maintaining a 24-Hour Service for Combating High-Tech Crime’, 25 June 2001, OJ C 187, 3.7.2001, p. 5–6, [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32001H0703\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32001H0703(01)).

<sup>107</sup> European Parliament, ‘Resolution of Parliament of the 19th of May 2002 Calling for Legislative Measures Against High-Tech Crime’, 19 May 2002.

<sup>108</sup> Council of the European Union and European Parliament, ‘Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency’, 077 OJ L § (2004), <http://data.europa.eu/eli/reg/2004/460/oj/eng>.

<sup>109</sup> Council of the European Union, ‘Common Position (EC) No 39/2003 of 26 May 2003 Adopted by the Council, Acting in Accordance with the Procedure Referred to in Article 251 of the Treaty Establishing the European Community, with a View to Adopting a Decision of the European Parliament and of the Council

The new agency would play a key role in coordinating and disseminating new knowledge and good practices in the field of security, assisting in the development of future Union policies<sup>110</sup>. In fact, the evaluation of the overall strategy stressed this as one of the most important progresses. The emphasis on security could be grasped through the rapid agreement behind the creation of ENISA<sup>111</sup>.

At the same time all the Member States had implemented the electronic signature directive and were aiming to the implementation of measures to secure transactions<sup>112</sup>.

The European Commission welcomed both the positive report of the MODINIS programme and of final eEurope 2005 assessment, confirming their effectiveness and utility<sup>113</sup>. Despite this, the first cracks were already beginning to appear in the framework of the plan<sup>114</sup>.

### II.2.3 i2010 strategy (2005-2010)

The next and last part of the analysis of the decade is dedicated to the so-called i2010 strategy, which surpassed its precedent in length, covering the last five years. During this span of time European society was fully experiencing the effects of the digitisation of contents. “The digital convergence of information society and media services, networks and devices [was] finally becoming an everyday reality”. Therefore, the European Union needed to continue to foster innovations, introducing innovative policies. “Digital convergence require[d] policy convergence and a willingness to adapt regulatory frameworks where needed so they are consistent with the emerging digital economy”<sup>115</sup>. The new approach was to integrate security as a technological enabler for the main priorities of the plan.

In particular, the creation of a Single European Information Space couldn’t stand the lack of security, which was the prerequisite for the trust of investors and consumers. This brought to the gradual introduction of a consistent system of rules, that encompassed also electronic

---

Adopting a Multiannual Programme (2003 to 2005) for the Monitoring of the eEurope 2005 Action Plan, Dissemination of Good Practices and the Improvement of Network and Information Security (MODINIS)’, 6.

<sup>110</sup> Alfonso Contaldo, ‘L’ENISA e Le Competenze Comunitarie per La Cibersicurezza’, *Rivista Di Polizia*, no. 6–7 (2018): 655–81.

<sup>111</sup> European Commission, ‘Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - eEurope 2005 Mid-Term Review’, 18 February 2004, 8, COM/2004/0108 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52004DC0108&qid=1685698009806>.

<sup>112</sup> European Commission, ‘Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - eEurope 2005 Action Plan: An Update {SEC(2004) 607} {SEC(2004) 608}’, 17 May 2004, 13–14, COM/2004/0380 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52004DC0380&qid=1685698009806>.

<sup>113</sup> European Commission, ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Final Evaluation of the eEurope 2005 Action Plan and of the Multiannual Programme (2003-2006) for the Monitoring of eEurope 2005 Action Plan, Dissemination of Good Practices and the Improvement of Network and Information Security (Modinis)’, 7.

<sup>114</sup> The first analyses of the strategy started to highlight how many of its objectives were going to not be accomplished. Notwithstanding the general agreement about the goals, the needed reforms were far from being implemented. See Guido Tabellini and Charles Wyplosz, ‘Supply-Side Reforms in Europe: Can the Lisbon Strategy Be Repaired?’, *Swedish Economic Policy Review* 1, no. 13 (2006): 101–56.

<sup>115</sup> European Commission, ‘Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - “i2010 – A European Information Society for Growth and Employment”’, 1 June 2005, 3, COM(2005) 229 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52005DC0229>.

communication, as an example of best practice for effectively opening to competition.

Although telecoms were always a priority together with their swift and through transposition, other topics were being valorised by EU politics. Cybercrime were one of the recurring priorities of those years and was starting to emerge with the passage from simple meta-governance to actual introduction of the first legal frameworks.

The Council Framework Decision on attacks against information systems<sup>116</sup> was the first real attempt towards a more robust legal layer for prosecution, improving judicial cooperation through approximation of national law rules. The framework embodied the general agreement on some general definition for cyberattacks to outline a common ground about what can be deemed as an illegal activity.

The same goal was shared by the parallel Council decision on sexual exploitation of children and child pornography<sup>117</sup>, even though only some minimum requirements were set across member states.

Notwithstanding the initial results, “the security as resilience logic behind these framework decisions though was to make cooperation and coordination of efforts easier among the relevant public authorities, even if in practice there remained constraints given that there was no real culture of security that underpinned them”<sup>118</sup>.

Supporting the introduction of such culture was one of the objectives of the European Commission, which in fact decided to adopt a communication about the state of ICT in the Union to update the previous proposal for a European policy approach. The communication “reviews the current state of threats to the security of the Information Society and determines what additional steps should be taken to improve network and information security (NIS)”<sup>119</sup>. It consents to capture the main priorities about security, which were a persistent topic for the decade in discourse. It is possible to find other milestones in the introduction of specific network and information security measures or in the improvement of the already recalled telecom regulation, whose evolution was shifting from a mere technical market intervention to a more specific security-related provisions, compelling providers to prioritize the safeguard of their users<sup>120</sup>.

The establishment of a shared “security culture” required a new level of coordination, which was finding both internal and international support. While from the internal side, ENISA’s contribution must be recognized, the external action of EU concerned different stakeholders, from the Organisation for Economic Co-operation and Development to the

---

<sup>116</sup> Council of the European Union, ‘Council Framework Decision 2005/222/JHA of 24 February 2005 on Attacks against Information Systems’ (2005), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32005F0222&qid=1659969013825>.

<sup>117</sup> Council of the European Union, ‘Council Framework Decision 2004/68/JHA of 22 December 2003 on Combating the Sexual Exploitation of Children and Child Pornography’, 013 OJ L § (2003), [http://data.europa.eu/eli/dec\\_framw/2004/68/oj/eng](http://data.europa.eu/eli/dec_framw/2004/68/oj/eng).

<sup>118</sup> Christou, ‘The European Union and Cybercrime’, 93.

<sup>119</sup> European Commission, ‘Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - A Strategy for a Secure Information Society - “Dialogue, Partnership and Empowerment”’, 31 May 2006, 3, COM(2006) 251 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52006DC0251&qid=1683984996443>.

<sup>120</sup> III.1.1 paragraph will be dedicated to further explanation of telecom discipline from the point of view of the security measures.

United Nations. In particular, the World Summit on the Information Society<sup>121</sup> was the setting in which the European Union supported ICT security, bringing attention on the next steps: “the need to continue the fight against cybercrime and spam while ensuring the protection of privacy and freedom of expression”. To achieve these purposes, the global community affirmed the need to pool knowledge on security.

That was the only viable solution to face the challenges coming from the new technological possibilities. Although cybercrime was still a relatively new emerging category of crime with only few agreed common definitions, many reports and studies were stressing the direct proportion between the phenomenon and the increase of connectivity<sup>122</sup>, which was making that type of business more and more profitable. Cybercrime was on the rise and was rapidly evolving, honing its set of techniques, that most of the times coincided with an innovative typology of malware<sup>123</sup>.

The whole scenario was further complicated by the rapid emergence of new and small devices, which were contributing to the theorization of the concept of “ambient intelligence”, as it was referred to by the European Commission<sup>124</sup>. Even if the level of development was

---

<sup>121</sup> The World Summit on the Information Society (WSIS) was a two-phase United Nations-sponsored conferences and summits that aimed to address global issues of information and communication technologies (ICTs) and their impact on society and the economy. The first phase of the summit, WSIS I, was held in 2003 in Geneva, Switzerland, and it was considered the first-ever international gathering on ICTs. The central themes of WSIS I were bridging the digital divide between developed and developing countries and promoting the use of ICTs to achieve sustainable economic and social development. The second phase of the summit, WSIS II, was held in 2005 in Tunis, Tunisia. During WSIS II, the participants reviewed what had been achieved under the Geneva Plan of Action and adopted the Tunis Commitment and the Tunis Agenda for the Information Society. The Tunis Commitment reiterated the need to build inclusive and accessible information societies, while the Tunis Agenda outlined the strategies and mechanisms for the implementation of various ICT-related objectives, such as infrastructure development, access to information, and capacity-building. Together, the two phases of the WSIS established a framework for global cooperation on the development of ICTs and their role in promoting economic and social development. ‘World Summit on the Information Society’, accessed 17 June 2023, <https://www.itu.int/net/wsis/>.

<sup>122</sup> The Computer Security Institute (CSI) was a professional organization of professionals in network and computer security founded in 1974, which was famous for its Annual Computer Security Conference. The event was usually organized with the cooperation of FBI and captured the main trends about cybercrime. The conference held in 2006 showed how the threat from computer crime and other information security breaches was real. Unauthorized accesses, thefts of proprietary information, and identity thefts were only some of the results emerging from the last survey, which identified viruses as the “greatest financial losses, accounting for 32 percent of the overall losses reported”. See ‘10th CSI/FBI Survey Shows Cybercrime Losses Down For Fourth Straight Year’, accessed 17 June 2023, <https://www.crime-research.org/news/26.01.2006/1786/>; ‘Computer Security Institute’, in *Wikipedia*, 24 March 2023, [https://en.wikipedia.org/w/index.php?title=Computer\\_Security\\_Institute&oldid=1146421118](https://en.wikipedia.org/w/index.php?title=Computer_Security_Institute&oldid=1146421118).

<sup>123</sup> The crisis caused by the Dos attacks against Estonia was a perfect example of the EU realisation of the broad capacities of advanced persistent threats. The attack was attributed to Russia and explained as a retaliation for the relocation of a Soviet monument from the centre of Tallinn. Extensive damages were caused since many companies and entities were forced to shut down their activities. As a result of the mitigation Estonia was temporarily isolated from the rest of the world. See Mark Landler and John Markoff, ‘Digital Fears Emerge After Data Siege in Estonia’, *The New York Times*, 29 May 2007, sec. Technology, <https://www.nytimes.com/2007/05/29/technology/29estonia.html>; Ian Traynor, ‘Russia Accused of Unleashing Cyberwar to Disable Estonia’, *The Guardian*, 17 May 2007, sec. World news, <https://www.theguardian.com/world/2007/may/17/topstories3.russia>.

<sup>124</sup> European Commission, ‘Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - A Strategy for a Secure Information Society - “Dialogue, Partnership and Empowerment”’, 5.

not comparable with the modern Internet of Things (IoT), there was concern about ensuring that the right conditions for openness and interoperability were in place, in order to avoid closures in platforms and applications, which would otherwise compromise security.

Then as now “a breach in NIS can generate an impact that transcends the economic dimension”<sup>125</sup>, but the consequences were masked by the contradiction of a poor return from the investments in security, that was not an appealing feature for users, who at the same time were also unaware of their responsibilities.

Since “NIS should [have been] presented as a virtue and an opportunity rather than as a liability and a cost [...] the key challenge for policy makers [was] to achieve a holistic approach”, recognizing the roles of all the stakeholders, and exploiting ENISA’s capabilities<sup>126</sup>.

This premise explains the dynamic and integrated multi-stakeholders approach proposed by the Commission, which was outlined into different initiatives to attain an efficient exploitation of information about security. A better use of this knowledge is the reason of the discussion about the future amendments of the framework about electronic communications, among which there was the proposal of a mandatory notification of incidents concerning telecom providers. However, the problem was about the lack both of proper incentives for new products and services for security and of a proper infrastructure for information sharing and alerting.

The latter initiative was evidence of the increasing focus on critical infrastructures, in parallel with the wave of terroristic attacks that had also involved Europe. From this point of view, infrastructures security can be seen as the other face of cybercrime, especially of its most extreme instance.

While the first legislative interventions were about online contents, the subsequent others started to focus on other types of offence. The battle against terrorism required the swift implementation of new instruments which had to consider the new digital ecosystem. All these requirements can be resumed with the word resilience. It is not a coincidence that the term which had been disregarded in the policies of the nineties became of the utmost importance during the next decade, taking into account the development, but also the inherent interconnections that was characterising infrastructures<sup>127</sup>.

Not only the 2004 was the year of “the deadliest terrorist attack on a European target since World War II”<sup>128</sup>, but was also the turning point for a European awareness about the severity of the problem. European institutions revised a plan of action for combatting terrorism,

---

<sup>125</sup> European Commission, 5.

<sup>126</sup> European Commission, 6.

<sup>127</sup> Chris Zebrowski and Daniel Sage, ‘Resilience and Critical Infrastructure: Origins, Theories, and Critiques’, in *The Palgrave Handbook of Security, Risk and Intelligence*, ed. Robert Dover, Huw Dylan, and Michael S. Goodman (London: Palgrave Macmillan UK, 2017), 1–4, [https://doi.org/10.1057/978-1-137-53675-4\\_7](https://doi.org/10.1057/978-1-137-53675-4_7). The authors take the example of two US documents, a report from the Presidential Commission on Critical Infrastructure Protection of 1997 and the Presidential Policy Directive n. 21 (“Critical Infrastructure Security and Resilience”) of 2013. While the word resilience appears just four times in the first document, it appears forty-four times in the second one. If in the first case the meaning could be described as a synonym for the term robustness, the second document showed a more modern description: “ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions”.

<sup>128</sup> Elaine Sciolino, ‘Spain Struggles to Absorb Worst Terrorist Attack in Its History’, *The New York Times*, 11 March 2004, sec. World, <https://www.nytimes.com/2004/03/11/international/europe/spain-struggles-to-absorb-worst-terrorist-attack-in-its.html>.

identifying a number of priorities among which there was the prevention of attacks through a better protection of critical infrastructures.

That was the preamble to an integrated approach in the fight against terrorism, using the whole available EU instruments, from external action to law enforcement cooperation<sup>129</sup>.

The sanction of the Hague program in 2005 by EU Council represented the right synthesis of the previous efforts, confirming the European will to fight against terrorists<sup>130</sup>.

Although the concept of critical infrastructure remains evanescent to the present, due to the interdependency with different sectors<sup>131</sup>, some elements for a botched definition can be found in the convention of UN, which underlined the connection between criminal law, data availability policies, and those structures on which society stands<sup>132</sup>.

The fright of the cascade effects a terroristic attack could cause, enticed the European Commission to identify some criteria to define critical infrastructures, considering the scope, as the geographic area served by the target infrastructure, the magnitude of the incident, taking into account different profiles of damage (economical, political, environmental, etc.), and the effects of time, as the point in time from which the loss would start having a serious impact.

These principles were condensed into the following definition, which can be appreciated for its broadness: "Critical infrastructures consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States"<sup>133</sup>.

Acknowledging the limits of the European action, due to the subsidiarity principle that limits EU intervention to the protection of transboundary infrastructures, Member states were urged to identify their criticalities and dependencies, keeping an up-to-date database, exchanging alerts' information, and guaranteeing the adoption of an appropriate security level. Notwithstanding the restricted scope, the European Programme for Critical Infrastructure Protection provided important support, that was translated into the implementation of uniform sectorial standards, thanks to the work of the European Committee for Standardization (CEN).

To endorse the successful accomplishment of the framework the European Commission collected feedback on policy options and best practices to jointly steer its development.

---

<sup>129</sup> European Commission, 'Communication from the Commission to the Council and the European Parliament - Prevention, Preparedness and Response to Terrorist Attacks', 20 October 2004, 5–9, COM/2004/0698 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52004DC0698>.

<sup>130</sup> Council of the European Union, 'The Hague Programme: Strengthening Freedom, Security and Justice in the European Union', 3 March 2005, 7–8, 2005/C 53/01, [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52005XG0303\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52005XG0303(01)).

<sup>131</sup> Jakub Harašta, 'Legally Critical: Defining Critical Infrastructure in an Interconnected World', *International Journal of Critical Infrastructure Protection* 21 (June 2018): 48–51, <https://doi.org/10.1016/j.ijcip.2018.05.007>.

<sup>132</sup> UN General Assembly, 'Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures :: Resolution /: Adopted by the General Assembly' (UN, 30 January 2004), 3, <https://digitallibrary.un.org/record/509571>.

<sup>133</sup> European Commission, 'Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the Fight against Terrorism', 20 October 2004, 3, COM/2004/0702 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52004DC0702&qid=1685943519045>.



Although the general purpose was sufficiently clear, all the details were under discussion at the start. Even the scope of the hazard approach was undefined, being influenced by the origins of the legislation, which can be traced back to the escalation of the terrorist phenomenon. In fact, among the different approaches there was also the option of focusing on terrorism only, neglecting other and more common threats.

Despite that initial openness of the discussion, the scope assumed soon a broader posture to encompass all hazards from the threat from intentional attacks to the threat from natural disasters.

The goal was to “to ensure that there are adequate and equal levels of protective security on critical infrastructure, minimal single points of failure and rapid, tested recovery arrangements throughout the Union”, minimising any negative impact of security investments on competitiveness<sup>134</sup>.

The mitigation of the drawbacks was guided by the affirmation of some principles. Apart from the already mentioned subsidiarity of the intervention, which is first and foremost a national responsibility, the principles of cooperation and complementarity draws the vertical approach at the bedrock. Not only all the members states have to cooperate, but cooperation has also to be seen upwards with European institutions and downwards with all business operators and even the single users. At the same time the new measures must be put in a synergic context with all the others existing regulations, while the proportionality principle remains at the end of the system. It remembers how infrastructures cannot be protected from all threats, but a risk-based approach has to be privileged.

This focus on improving the average security can be explained by the fact that “protection measures are only as strong as their weakest link”<sup>135</sup>, due to the existent interconnection between infrastructures. Therefore, having some peaks of protection is useless, as long as there are less protected spots.

It deserves to be remarked how the virtuous implementation of the regulation was the result of a free choice of the member states. The most of them decided to implement the framework even for national critical infrastructure, applying national legislations that were coherent with the overall European plan. In this way national authorities weren’t only a mere point of contact, but real guarantors. This was proof of greater integration, but also of the strength of the multi-stakeholder approach that was being adopted for digital.

On that basis, the European Commission improved its efforts, exploiting the feedback received from the single states, and confirming its goal to push forward with the information exchange, both by establishing groups of experts, and by integrating its ARGUS system with a dedicated Critical Infrastructure Warning Information Network (CIWIN)<sup>136</sup>.

---

<sup>134</sup> European Commission, ‘Green Paper on a European Programme for Critical Infrastructure Protection’, 17 November 2005, 3, COM/2005/0576 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52005DC0576>.

<sup>135</sup> European Commission, 5.

<sup>136</sup> European Commission, ‘Communication from the Commission on a European Programme for Critical Infrastructure Protection’, 12 December 2006, 5–6, COM(2006) 786 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52006DC0786&qid=1687081895752>. After its announcement in a communication against terrorism in 2004, the general rapid alert system (ARGUS) became operational on 1 January 2006. The official proposal by European Commission for its introduction underlined the need for an enhancement in European coordination in front of both natural and man-made crises. From this point of view, the supporting role of the Commission was an example of a renewed European solidarity principle both between

Regarding all these interventions, it must be stressed how the legal basis was always the same. Both the Council directive on critical infrastructures<sup>137</sup> and the proposal for the CIWIN recalled art. 308 of the Treaty establishing the European Community, which aims to provide European institutions with the necessary powers to accomplish the goal of a common market. Even if a different awareness of threats was taking root, the constant of the common market remained that flexible instrument which was utilized to expand European scope of action. Even so there was a fundamental difference in comparison with the nineties. While before the market had been both an end and a means, during the first decade it finally became a mean for a nobler purpose, that European solidarity against the common threat of terrorism in all its forms.

As further evidence, the effects of this change could be seen in the choices of the European lawmaker. From critical infrastructures and cybercrime to electronic communications, the approach acknowledged the severity of the threat made possible by digital transformation and answered by making security a focal point. Although the policies were struggling to show the first concrete results<sup>138</sup>, a change of pace can be seen in the comprehensive adaptation

---

member states and between European institutions and member states. ARGUS consists of an internal communication network and a specific coordination process to be activated in case of a major multisectoral crisis, as defined in the Commission's internal rules of Procedure. Although it showed its limitations, it was deployed during the recent pandemic, it made clear the need for an "EU crisis dashboard". The idea was to complement this base with an infrastructure dedicated to critical information sharing between member states to compensate the initial lack of minimum and horizontal standards. See European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Commission Provisions on "ARGUS" General Rapid Alert System', 2005, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52005DC0662&qid=1687593795069>; 'All News - European Commission', accessed 24 June 2023, <https://drmkc.jrc.ec.europa.eu/events-news/all-news#details21159>; 'Critical Infrastructure Warning Information Network (CIWIN)', accessed 24 June 2023, [https://home-affairs.ec.europa.eu/networks/critical-infrastructure-warning-information-network-ciwin\\_en](https://home-affairs.ec.europa.eu/networks/critical-infrastructure-warning-information-network-ciwin_en); European Commission, 'Proposal for a Council Decision on a Critical Infrastructure Warning Information Network (CIWIN) {SEC(2008)2701} {SEC(2008)2702}' (2008), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52008PC0676&qid=1687594552943>.

<sup>137</sup> Council of the European Union, 'Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection', Pub. L. No. 345, OJ L (2008), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114>. For a more comprehensive explanation of the regulation in the light of the recent European reform of critical infrastructures see III.1.3.

<sup>138</sup> The approach to security was surely different, but the policies of the Lisbon Strategy did not have any important positive effect. The interventions represented a starting point but could not make a huge difference. For example, the regulations against cybercrime were facing a sophistication of criminal activities, which were growing around organized groups. While the phenomenon was more and more relevant, "the number of European prosecutions on the basis of cross-border law enforcement cooperation do not increase". See European Commission, 'Communication from the Commission to the European Parliament, the Council and the Committee of the Regions - Towards a General Policy on the Fight against Cyber Crime {SEC(2007) 641} {SEC(2007) 642}', 22 May 2007, 3, COM(2007) 267 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52007DC0267&qid=1684082047897>. Regarding critical infrastructures, different issues were still lingering. First, national approaches were adopting very different measures and regimes, also due to the lack of expertise of many countries. Proper integration was missing as a consequence of the poor involvement of the private sector, which owns the most of the national critical infrastructures. Member states would have had to foster the creation of public-private partnerships (PPPs). Second, cooperation and information sharing were still underdeveloped and monitoring practices differed significantly across Member States. See European Commission, 'COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF

of the rules to both introduce security measures and producing useful security-related information.

Although the dichotomy rights and security apparently seems to be connected by a directly proportional relationship, many cases often contributed to shedding light and shadow. In fact, among the different contrasts in the literature there is that between privacy and security, which since ancient times, even before the first developments of the modern computer science, have characterized the relationship between the individual and the State. “Cybersecurity measures at the national level may create a condition of discrimination by affecting people’s access to some resources or services, have economic implications that affect fairness, influence freedom of expression, limit people’s autonomy and violate privacy”<sup>139</sup>.

In particular, the privileged access by governments to ICT services for law enforcement purposes, may endanger pivotal values for contemporary societies. An example of that had been the renown data retention directive, which was the root cause for a famous series of lawsuits of the European Court of Justice<sup>140</sup>.

As it has been remarked, data exchange is a prime requirement for an effective response to cyber-attacks, but sometimes efficiency comes at a cost, which was in the peril of a surveillance society. States must win the resistance by private operators to disclose their information, but the manner in which this trespass occurs inevitably cause a compression of fundamental rights.

“There is then a real tension between ensuring access for security, and preserving the privacy of personal data, which is embedded not just in the legal, but also the political and cultural dimension of achieving a politics of resilience”<sup>141</sup>.

The many inconsistencies behind the directive implementation raised the concerns of the data protection authorities in Europe. While the Article 29’s Working Party stressed the inherent risks for confidentiality and freedom of expression, the EDPS bluntly alleged the failure of the directive because data were not used only to combat serious crime. An

---

THE REGIONS on Critical Information Infrastructure Protection “Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience”, 30 March 2009, 5–7, COM/2009/0149 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52009DC0149>.

<sup>139</sup> Eleonora Viganò, Michele Loi, and Emad Yaghmaei, ‘Cybersecurity of Critical Infrastructure’, in *The Ethics of Cybersecurity*, ed. Markus Christen, Bert Gordijn, and Michele Loi, The International Library of Ethics, Law and Technology (Cham: Springer International Publishing, 2020), 158–63, [https://doi.org/10.1007/978-3-030-29053-5\\_8](https://doi.org/10.1007/978-3-030-29053-5_8).

<sup>140</sup> Since this is not the seat to properly discuss the topic, which would deserve more careful examination, I simply refer to the abundant literature. Darja Dusanovic, ‘Implications of Invalidity of Data Retention Directive to Telecom Operators’, *Juridical Tribune Journal = Tribuna Juridica* 4, no. 2 (2014): 44–60; Orla Lynskey, ‘The Data Retention Directive Is Incompatible with the Rights to Privacy and Data Protection and Is Invalid in Its Entirety: Digital Rights Ireland’, *Common Market Law Review* 51, no. 6 (2014): 1789–1811; Judith Rauhofer and Daithí Mac Síthigh, ‘The Data Retention Directive Never Existed’, *SCRIPTed* 11, no. 1 (2014), <https://doi.org/10.2966/scrip.110114.118>; Xavier Tracol, ‘Legislative Genesis and Judicial Death of a Directive: The European Court of Justice Invalidated the Data Retention Directive (2006/24/EC) Thereby Creating a Sustained Period of Legal Uncertainty about the Validity of National Laws Which Enacted It’, *Computer Law & Security Review* 30, no. 6 (2014): 736–46, <https://doi.org/10.1016/j.clsr.2014.09.008>; Arianna Vidaschi and Valerio Lubello, ‘Data Retention and Its Implications for the Fundamental Right to Privacy: A European Perspective’, *Tilburg Law Review* 20, no. 1 (2015): 14–34, <https://doi.org/10.1163/22112596-02001005>; Sarah Tracey, ‘The Fall of the Data Retention Directive’, *Communications Law* 20, no. 2 (2015): 53–55.

<sup>141</sup> Christou, ‘The European Union and Cybercrime’, 96.

instrument that introduces rules for data retention should have also limited law enforcement access and further use. The evaluation report of the European Commission confirmed that view. Although the statistics showed how metadata are an effective tool in combatting crime, the final assessment set off an uneven condition of the transposition, accompanied by the incapability of prevent an unrespectful use of personal data<sup>142</sup>.

In the words of the European Digital Rights association: “More than five years after the Data Retention Directive was adopted, both the evaluation report of the European Commission and the shadow report of European Digital Rights show that the Directive has failed on every level. It has failed to respect the fundamental rights of European citizens, it has failed to harmonise the single market and has proven to be unnecessary to fight serious crime”<sup>143</sup>.

Notwithstanding the undisputable violation of fundamental rights, the directive was another proof of an ongoing urge that European institutions needed to satisfy, even at cost of reshaping existent frameworks of rules. Those amendments built upon the previous rules became the bedrock that paved the way for the onset of a more coherent and integrated securitisation process, a securitisation that was no more bound to the market, but that was a reaction to the insecurity that was marking the new millennium.

### II.3 Ten years to the present: from the failure of the strategy to modern cybersecurity

Both the mid-term and the final evaluation of i2010 strategy confirms the important contribution of information society and media policies to the achievement of the Lisbon goals, as well as the validity of i2010 as the reference framework for European information society and media policies<sup>144</sup>. “The achievements of i2010 and the ways it has been implemented in the Member States provide a snapshot of the dynamism and range of schemes that innovative policies can produce. i2010 has laid the building blocks for a modern ICT-enabled society”<sup>145</sup>.

While urging the draft of a new agenda, Europe appreciated that the building blocks for a modern ICT society had been put in place. Although that was the truth, the policies merely scratched the surface of the problems, which were running faster than solutions.

In 2009, a year before the definite conclusion of the strategy, an interview of Fredrik Reinfeldt, the Swedish Prime Minister who was holding the rotating EU Presidency, even declared the failure of the plans<sup>146</sup>.

---

<sup>142</sup> European Commission, ‘REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)’, 18 April 2011, 28–32, COM(2011) 225 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52011DC0225&qid=1685080832916>.

<sup>143</sup> European Digital Rights, ‘Shadow Evaluation Report on the Data Retention Directive (2006/24/EC) 17 April 2011’ (Bruxelles: European Digital Rights, 17 April 2011), 20–22, [https://edri.org/files/shadow\\_drd\\_report\\_110417.pdf](https://edri.org/files/shadow_drd_report_110417.pdf).

<sup>144</sup> European Commission, ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Preparing Europe’s Digital Future I2010 - Mid-Term Review {SEC(2008) 470}’, 17 April 2008, 12, COM/2008/0199 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52008DC0199&qid=1685802756502>.

<sup>145</sup> European Commission, ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Europe’s Digital Competitiveness Report : Main Achievements of the I2010 Strategy 2005-2009 {SEC(2009) 1060} {SEC(2009) 1103} {SEC(2009) 1104}’, 4 August 2009, 11, COM/2009/0390 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52009DC0390&qid=1685802756502>.

<sup>146</sup> ‘Sweden Admits Lisbon Agenda “failure” | EurActiv’, 3 June 2009,

Other commentators, however, insisted that this was an expected and predicted outcome.

"The ambitious Lisbon objectives of turning the EU into "the most dynamic, knowledge based economy in the world by 2010" are becoming an embarrassing joke. There is little or no sign that Europe's economic decline is stopping or turning around, particularly in the large countries of continental Europe. There is also substantial agreement on what should be done to improve the long run economic outlook, at least a general level. Yet, the economic reforms that are needed are not being implemented, or they are enacted too slowly. The Lisbon strategy is clearly failing"<sup>147</sup>

To summarise, even if the effort was unanimously supported by all EU governments, because the gap between Europe and the US was too wide in too many areas, the main "culprit" was an inherent lack of political will.

Despite this major shortcoming, the disgraceful outcome must be understood as the result of a more complex set of causes, which deserve a brief analysis.

Although structural reforms were needed, the adoption of the "open method of coordination" effectively prevented them from being implemented.

"This approach is based on the idea that there is a need for national governments to go further in these supply-side areas as well. Yet, it does not propose to centralize national policies"<sup>148</sup>. It can be seen as a flexible way of co-ordinating where there is no general agreement on centralisation. While the approach may be supportable for the labour market, where reforms should be undertaken by individual national governments, centralisation would have been the most appropriate method for the single market, where several internal barriers needed to be removed.

Basically, these were competences that were not directly attributed to the Union, but left to the individual Member States, which were supposed to recognise them as being of common interest. Consequently, the pressure exerted by the obligation to produce an annual report on the results achieved was not sufficient.

On paper, at least, the assumptions for change through peer pressure were agreeable. In reality, relations between European countries are more complex than the European Commission imagined.

For example, while the economic development of one country can certainly trigger the development of others, there is also the possibility that most will simply enjoy the positive externality of increased demand for products.

On the other hand, political pressure from other countries also needs to be reduced. Indeed, it is clear that all Member States share the problem of having to deal with their internal lobbies, which are one of the first obstacles to reform.

The effect has been to turn peer pressure into mutual congratulations, each succumbing to the flattery of its electorate, and to make the European Commission's control excessively diplomatic<sup>149</sup>.

---

<http://web.archive.org/web/20110609124031/http://www.euractiv.com/en/priorities/sweden-admits-lisbon-agenda-failure/article-182797>.

<sup>147</sup> Tabellini and Wyplosz, 'Supply-Side Reforms in Europe: Can the Lisbon Strategy Be Repaired?', 1.

<sup>148</sup> Tabellini and Wyplosz, 1.

<sup>149</sup> 'The Failure of the Lisbon Strategy', CEPR, 12 January 2010, <https://cepr.org/voxeu/columns/failure-lisbon-strategy>.

At the very least, however, the strategy can be viewed in terms of its great information production. Despite the poor results, the ongoing meetings and associated reporting provide an important wealth of information on which to base subsequent reforms, with comparisons to the level of development achieved by other countries.

Nevertheless, the strong criticism of the strategy must be acknowledged. Not only has it been accused of creating a useless bureaucracy, but it has also been hoped for its final demise: “I hope that in two months the Heads of State and Government let the Lisbon strategy die a peaceful death”<sup>150</sup>.

### II.3.1 Europe 2020

Admitting failure did not stop Europe's innovation efforts. Rather, it represented a new push for development, as the European Commission promoted a new initiative to compensate for all the previous efforts of the Lisbon Strategy.

“Europe faces a moment of transformation. The crisis has wiped out years of economic and social progress and exposed structural weaknesses in Europe's economy. In the meantime, the world is moving fast and long-term challenges – globalisation, pressure on resources, ageing – intensify. The EU must now take charge of its future. [...]

We need a strategy to help us come out stronger from the crisis and turn the EU into a smart, sustainable and inclusive economy delivering high levels of employment, productivity and social cohesion. Europe 2020 sets out a vision of Europe's social market economy for the 21st century”<sup>151</sup>.

With its usual self-confidence, the Union set itself almost the same goals as it had set itself for the previous decade. The only thing that had changed was the pace of the rest of the world, which was accelerating. To keep up, the Commission identified three priorities, which can be summed up in a single word: growth.

This growth needs to be smart, sustainable and inclusive, in order to develop research, the green economy and social cohesion at the same time.

That is why seven flagship initiatives were outlined to support progress, each with its own agenda and remit. Among them, Europe 2020 introduced a Digital Agenda for Europe, which focused on the digitisation process of the Union.

Similar to what was hoped for in the past, the main interventions concerned the improvement of telecommunications infrastructures, in particular the Internet infrastructure, to increase both its available speed and its penetration.

On the other hand, improved access should have been accompanied by the right conditions for its exploitation. A true single market for online content and services, without internal barriers, would have provided a fertile ground for the spread of European cultural heritage and shaped the governance of the Internet accordingly.

The idea has always been to create a virtuous circle between increased Internet access and the creation of new content. In this way, the investment would have benefited the positive externalities of other areas, maximising the results.

Clearly, the success of the initiative depended on the existence of appropriate support for digital literacy, as well as a reduction in the cost of network roll-out. Only these requirements

---

<sup>150</sup> ‘The Failure of the Lisbon Strategy’.

<sup>151</sup> European Commission, ‘EUROPE 2020 - A Strategy for Smart, Sustainable and Inclusive Growth’, 3 March 2010, 5, COM/2010/2020 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52010DC2020>.

would have made it possible for countries to implement and use modern, accessible online services for e-government and e-health<sup>152</sup>.

In essence, this was an important endorsement of the future path, even if it was not an innovative endeavour, as most of the points merely recalled the previous strategy. The legacy of the last decade required a change in instruments and methodologies, but the substance was unchanged, and the EU institutions were committed to its ideal completion.

As a specific policy for digitisation, the Digital Agenda provided the essential blueprint for an EU strategy in the digital age. "The development of the digital single market and the prosperity of European economies depended on gaining users' confidence and trust in cyberspace and digital services"<sup>153</sup>.

If the final objective was "to deliver sustainable economic and social benefits from a digital single market based on fast and ultra-fast internet and interoperable applications"<sup>154</sup>, this can be seen as an ideal mix of the Union's competences for the internal market and for the area of freedom and security, as their achievements had to be synergised to support the digitisation process.

In a market where "Europe is still a patchwork of national online markets"<sup>155</sup>, the only solution was to create the conditions for the circulation of content in order to attract new investment, thus creating a virtuous circle, as has already been stressed. But this self-sustaining force would only work in a secure environment. "Europeans will not embrace technology they do not trust - the digital age is neither "Big Brother" nor the "cyber Wild West"<sup>156</sup>.

The objective of building an area of freedom, security and justice on the achievements of the Tampere and Hague programmes can therefore be seen as a synergistic initiative to help address this lack of public confidence. "In spite of these and other important achievements in the area of freedom, security and justice Europe still faces challenges. These challenges must be addressed in a comprehensive manner. Further efforts are thus needed in order to improve coherence between policy areas"<sup>157</sup>.

Under this policy umbrella, the main objective was to continue the fight against cybercrime and terrorism, as started a decade earlier, but to promote the development of European solidarity in order to make full use of art. 222 TFEU, which can be seen as the key to the internal security strategy.

There was "a need for a horizontal and cross-cutting approach to deal with complex crises

---

<sup>152</sup> European Commission, 14.

<sup>153</sup> Kadri Kaan Renda, 'THE DEVELOPMENT OF EU CYBERSECURITY POLICY: FROM A COORDINATING ACTOR TO A CYBER POWER?', *Ankara Avrupa Calismalari Dergisi*, 2022, 476.

<sup>154</sup> European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Agenda for Europe', 19 May 2010, 3, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52010DC0245&qid=1683010781997>.

<sup>155</sup> European Commission, 5.

<sup>156</sup> European Commission, 16.

<sup>157</sup> Council of the European Union, 'The Stockholm Programme — An Open and Secure Europe Serving and Protecting Citizens', 4 May 2010, 5, 2010/C 115/01, <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:EN:PDF>.

or natural or man-made disasters"<sup>158</sup>. In fact, the possibility of sharing high quality data would have complemented both the cybercrime and critical infrastructure efforts.

As a result, a new wave of European cooperation took place with the establishment of a European Cybercrime Centre at Europol<sup>159</sup> and the strengthening of Computer Emergency Response Teams (CERTs) in Europe.

ENISA, whose mandate had recently been renewed<sup>160</sup>, was an essential point of reference, not only for defining and disseminating good practices for the organisation of CERTs, but also for accompanying other legislation.

Reference can be made to the efforts made in the field of telecommunications, where the reform of the second telecom package was a key element. "That revision [...] made mandatory [...] the reporting of any network and information systems security breaches to the national regulatory authority (NRA). This step-change was a significant (framing) move away from the voluntary approach [...], with ENISA tasked to support Member States in implementing Article 13a through the Technical Guidelines on Incident Reporting, which created a standard incident reporting methodology and mechanism"<sup>161</sup>.

This development has not been confined to the Union, as the agenda, and the Digital Single Market in particular need an external face because progress on many of the policy issues can

---

<sup>158</sup> Council of the European Union, 18.

<sup>159</sup> Over the years, Europol had begun to play an increasing role in the fight against cybercrime, gaining a progressive prominence that allowed it to influence European crime policy. See Rachel Woodward, 'Establishing Europol', *European Journal on Criminal Policy and Research* 1, no. 4 (December 1993): 7–33, <https://doi.org/10.1007/BF02249463>; Helena Carrapiço and Florian Trauner, 'Europol and Its Influence on EU Policy-Making on Organized Crime: Analyzing Governance Dynamics and Opportunities', *Perspectives on European Politics and Society* 14, no. 3 (September 2013): 357–71, <https://doi.org/10.1080/15705854.2013.817804>; Gregory Mounier, 'Europol: A New Player in the EU External Policy Field?', *Perspectives on European Politics and Society* 10, no. 4 (December 2009): 582–602, <https://doi.org/10.1080/15705850903314841>.

<sup>160</sup> Since its creation, ENISA has worked on the basis of a temporary mandate, which has been renewed until recently. After various amendments to the original regulation and its replacement by a new regulation in 2013, the so-called Cybersecurity Act signed its final nomination as the European Institution for Cybersecurity. This permanent appointment coincided with the formal renaming as the European Union Agency for Cybersecurity. For the legal references, please see European Parliament and Council of the European Union, 'Regulation (EC) No 1007/2008 of the European Parliament and of the Council of 24 September 2008 Amending Regulation (EC) No 460/2004 Establishing the European Network and Information Security Agency as Regards Its Duration', 293 OJ L § (2008), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008R1007>; European Parliament and Council of the European Union, 'Regulation (EU) No 580/2011 of the European Parliament and of the Council of 8 June 2011 Amending Regulation (EC) No 460/2004 Establishing the European Network and Information Security Agency as Regards Its Duration Text with EEA Relevance', 165 OJ L § (2011), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011R0580>; European Parliament and Council of the European Union, 'Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 Concerning the European Union Agency for Network and Information Security (ENISA) and Repealing Regulation (EC) No 460/2004', 165 OJ L § (2013), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013R0526>.

<sup>161</sup> George Christou, 'The Collective Securitisation of Cyberspace in the European Union', *West European Politics* 42, no. 2 (23 February 2019): 12, <https://doi.org/10.1080/01402382.2018.1510195>; European Union Agency for Cybersecurity, Marnix Dekker, and Christoffer Karsberg, 'Technical Guideline on Incident Reporting', 24 October 2014, <https://www.enisa.europa.eu/publications/technical-guideline-on-incident-reporting/@@download/fullReporthttps://www.enisa.europa.eu/publications/technical-guideline-on-incident-reporting/@@download/fullReport>.



only be made on an international level<sup>162</sup>.

All these needs, together with the issues that have emerged over the past decade, were crystallised by the European Commission into five priorities for the Internal Security Strategy, made possible by the new legal framework of the Treaty of Lisbon: "with the Treaty of Lisbon as the new legal framework, the Internal Security Strategy in Action should become the common agenda for the EU over the next four years"<sup>163</sup>.

Listing only those related to security, in its digital sense, makes it possible to further highlight the commitment to fight cybercrime and terrorism and to increase Europe's resilience to crises, which also implies a better protection of critical infrastructures, thus raising the average level of security.

"Our world is changing, and so are the threats and challenges around us. The response from the European Union should evolve correspondingly"<sup>164</sup>.

Although the fight against cybercrime remained a top priority, as demonstrated by the various initiatives developed with a view to harmonising criminal law<sup>165</sup>, "there [were] still several obstacles to the effective investigation of cybercrime and prosecution of offenders at European level"<sup>166</sup>.

Thus, "the European Commission has sought to improve cooperation and coordination among national law enforcement agencies and has promoted legal and political cooperation with third countries, with a particular emphasis on cybercrime training for law enforcement and judicial authorities"<sup>167</sup>. These objectives were also supported by the aforementioned foundation of the new European Cybercrime Centre.

It was in this scenario that the word "cybersecurity" began to be used by European institutions, along with other declensions. One of the first examples was a communication about critical infrastructures, which was accompanied by the title: "Towards Global Cybersecurity".

---

<sup>162</sup> European Commission, 'A Digital Agenda for Europe', 34.

<sup>163</sup> European Commission, 'Communication from the Commission to the European Parliament and the Council the Eu Internal Security Strategy in Action: Five Steps Towards a More Secure Europe', 22 November 2010, 16, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52010DC0673&qid=1683985600055>.

<sup>164</sup> European Commission, 16.

<sup>165</sup> European Commission, 'COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT Tackling Crime in Our Digital Age: Establishing a European Cybercrime Centre', 28 March 2012, COM/2012/0140 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52012DC0140&qid=1688740740533>. Although the main legal instrument to combat cybercrime has always been the Council of Europe Convention on Cybercrime, other regulatory measures are worth mentioning, such as the Directive on combating the sexual exploitation of children on the Internet and the Directive on attacks against information systems. See European Parliament and Council of the European Union, 'Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography, and Replacing Council Framework Decision 2004/68/JHA', 335 OJ L 5 (2011), <http://data.europa.eu/eli/dir/2011/93/oj/eng>; Council of the European Union and European Parliament, 'Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks against Information Systems and Replacing Council Framework Decision 2005/222/JHA' (2013), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013L0040>.

<sup>166</sup> European Commission, 'COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT Tackling Crime in Our Digital Age', 3.

<sup>167</sup> Christou, 'The Collective Securitisation of Cyberspace in the European Union', 17.

In fact, concerning the evolving threats against critical infrastructures, “we [were] witnessing a trend towards using ICT for political, economic and military predominance, including through offensive capabilities. ‘Cyber-warfare’ or ‘cyber-terrorism’ are sometimes mentioned in this context”<sup>168</sup>.

That resulted in international cooperation to establish common principles and guidelines for the resilience and stability of the Internet, as well as the first draft of ICT sector-specific criteria for identifying European Critical Infrastructures<sup>169</sup>.

Another time, as in the first period of telecommunications reform, “experience [showed] that purely national or regional approaches to security and resilience challenges [were] not enough”<sup>170</sup>.

This explains the renewal of ENISA's mandate and its modernisation to support Member States and EU institutions in their efforts, as also noted by the EU Council<sup>171</sup>.

### II.3.2 The 2013 Cybersecurity Strategy

While before 2009 “concerns about the single market and internal security shaped the EU’s approach toward cybersecurity in the 1990s and early 2000s”<sup>172</sup> the treaty of Lisbon produced a solid base for new institutional structures to finally address the issues coming from the expansion of the cyberspace. Due to the increasing activities of others global players, the EU was compelled to abandon its market-centred approach to really start acting in the cyberspace as a player. If the digital domain is a new surface of attack, the Union could not neglect the new arrays of threats implied by it.

The treaty of Lisbon “amended the Amsterdam and Maastricht Treaties and repackaged them as the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU)”<sup>173</sup> introducing a co-decision mechanism between the European Parliament and the EU Council, formalising its role as an official institution of the EU.

At the same time, the European Defence Agency was confirmed as a formal European body and the new European External Action Service (EEAS) started to assist the High Representative

---

<sup>168</sup> European Commission, ‘COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS ON Critical Information Infrastructure Protection “Achievements and next Steps: Towards Global Cyber-Security”’, 31 March 2011, 3, COM/2011/0163 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52011DC0163>.

<sup>169</sup> European Commission, 6.

<sup>170</sup> European Commission, 8.

<sup>171</sup> Council of the European Union, ‘Conclusions of the Council of the European Union on Critical Information Infrastructure Protection “Achievements and next Steps: Towards Global Cyber-Security”’, 19 May 2011, 7, <https://data.consilium.europa.eu/doc/document/ST-10299-2011-INIT/en/pdf>.

<sup>172</sup> Renda, ‘THE DEVELOPMENT OF EU CYBERSECURITY POLICY: FROM A COORDINATING ACTOR TO A CYBER POWER?’, 469.

<sup>173</sup> Robert S. Dewar, ‘Cyber-Lisbon? The Impact of the Treaty of Lisbon on European Union Cybersecurity Policy’, 2015, 1–6, <https://eustudies.org/conference/papers/download/107>. Before “this pillar structure was designed to formally separate economic and social dimensions of policy from more highly politicised areas”. The so-called “community method” was applied to the first pillar, where the European Commission held the monopoly of policy initiative and decisions were made by the Council using qualified majority voting. At the contrary the other two pillars implied the intergovernmental process, where the right of initiative was shared between the Commission and the Member States and the final approval needed the unanimously agreement of the EU Council.

of the Union for Foreign Affairs and Security Policy<sup>174</sup>.

More importantly, “the pillar system of policy development and implementation was abolished”<sup>175</sup>, enabling entities dealing with foreign affairs and internal market security, like agencies or Commission Directorates General, to work together with a holistic approach.

This explains why all the previous policy attempts were not fully successful because they were confined in a specific pillar, without the possibility to concern also defence or national security matters.

If the first phase before 2013 cybersecurity can be characterised as “mostly below the political radar”, the new European Cybersecurity Strategy paved the way towards a comprehensive and integrated EU cybersecurity policy<sup>176</sup>.

This necessity had already been advanced in a previous proposal on a European Strategy for Internet Security, which captured the centrality of digital technologies, nevertheless their increasing vulnerabilities. “Despite achievements made, the cyber-security capabilities within the EU [were] still not at the level which [was] necessary in order to ensure a high and efficient protection within the EU. Furthermore, most of the actions [were] carried out on a voluntary basis also considering that security is considered mainly to be a national prerogative. This [could] result in a lack of clear commitment by the Member States and stakeholders to deliver on those actions”<sup>177</sup>.

The year 2013 marked a steep change, with a focus on economic resilience. “The interrelationships between politics and economics suggest the need for combined soft and hard interventions for cybersecurity policy”<sup>178</sup>. This vision was perfectly captured in by the cybersecurity strategy.

“What the Cybersecurity Strategy did was to draw the elements together and enable the EU to move forward with a single strategic vision”<sup>179</sup>. Indeed, this is largely the logic pursued by the EU since 2013. “The new Strategy firmly established a unified position for the EU on cybersecurity”<sup>180</sup>.

Having recognized that cyberspace is a non-eliminable component of everyday life, the European Commission declared its intention to metaphorically colonize it to free it from any authoritarian drift.

“For cyberspace to remain open and free, the same norms, principles, and values that the EU upholds offline, should also apply online. Fundamental rights, democracy and the rule of law need to be protected in cyberspace”<sup>181</sup>. “Cybersecurity can only be sound and effective if

---

<sup>174</sup> Dewar, 11–12.

<sup>175</sup> Dewar, 2.

<sup>176</sup> Paul Timmers, ‘The European Union’s Cybersecurity Industrial Policy’, *Journal of Cyber Policy* 3, no. 3 (2 September 2018): 367, <https://doi.org/10.1080/23738871.2018.1562560>.

<sup>177</sup> European Commission, ‘ROADMAP - Proposal on a European Strategy for Internet Security’, November 2011, 2.

<sup>178</sup> Timmers, ‘The European Union’s Cybersecurity Industrial Policy’, 367.

<sup>179</sup> Dewar, ‘Cyber-Lisbon?’, 14.

<sup>180</sup> Dewar, 15.

<sup>181</sup> European Commission, ‘JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace’, 7 February 2013, 2, JOIN 1, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001>.

it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union and EU core values”<sup>182</sup>.

“But freedom online requires safety and security too. Cyberspace should be protected from incidents, malicious activities and misuse; and governments have a significant role in ensuring a free and safe cyberspace”<sup>183</sup>.

This is a shared responsibility that needs to be taken up by all relevant actors, both public and private, as recognized by the Commission: “Governments have several tasks: to safeguard access and openness, to respect and protect fundamental rights online and to maintain the reliability and interoperability of the Internet. However, the private sector owns and operates significant parts of cyberspace, and so any initiative aiming to be successful in this area has to recognise its leading role”<sup>184</sup>.

Despite the EU's attempt to address the problem comprehensively, the strategy sometimes seems to repeat a familiar story. The scenario is one of a steady increase in cyber-attacks, accompanied by the flourishing of cyber-crime and the misuse of technology by states for surveillance purposes. All these problems explain why “governments across the world have started to develop cybersecurity strategies and to consider cyberspace as an increasingly important international issue”<sup>185</sup>.

But a stronger and more coordinated response was called for on the EU level.

Five strategic priorities were proposed to address these issues: achieving cyber resilience, reducing cybercrime, developing a cyberdefence policy, fostering the development of industrial and technological resources for cybersecurity, and establishing a coherent international cyberspace policy for the entire European Union<sup>186</sup>.

The first issue can be seen as the ideal continuation of all the efforts to create a functional framework for critical infrastructures. Indeed, the term “resilience” is used to highlight the ability to “develop capabilities and cooperate effectively [...] to counter cyber risks and threats having a cross-border dimension [and a] coordinated response in emergency situations”<sup>187</sup>.

“Resilience is therefore the ability of a community or society to cope, adapt, and recover dangers to which it is exposed and its consequences in a timely and effective manner, thus preserving or rapidly restoring vital basic structures and basic functions”<sup>188</sup>.

The obligations arising from the combined application of the electronic communications and data protection frameworks and ENISA's oversight were cited as a virtuous example of what had already been achieved in building a European cybersecurity posture.

But there were still “gaps across the EU, notably in terms of national capabilities, coordination in cases of incidents spanning across borders”<sup>189</sup>.

---

<sup>182</sup> European Commission, 4.

<sup>183</sup> European Commission, 2.

<sup>184</sup> European Commission, 2.

<sup>185</sup> European Commission, 3.

<sup>186</sup> European Commission, 4–5.

<sup>187</sup> European Commission, 5.

<sup>188</sup> Andreas Düll, Anja Schoch, and Matthias Straub, ‘Cybersecurity in the European Union’, *Central and Eastern European eDem and eGov Days* 331 (12 July 2018): 2, <https://doi.org/10.24989/ocg.v331.26>.

<sup>189</sup> European Commission, ‘JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - Cybersecurity

The Commission therefore welcomed the proposal for the well-known NIS Directive to complete the picture by setting minimum requirements and procedures for information exchange and response to cross-border incidents.

The second issue addressed by the Commission was cybercrime, the sophistication of which had made this illegal activity a high-profit, low-risk business. The legal basis for combating this phenomenon had to be strengthened and enforced, since the directives had to be transposed and many countries had not yet ratified the Council of Europe's Budapest Convention on Cybercrime<sup>190</sup>.

Therefore, from the point of view of substantive criminal law, it was as if the basics were not evenly distributed across the European Union. On the other hand, progress was being made through the new and growing cooperation between European institutions, thanks to the new European Cybercrime Centre (EC3), which was "tasked with aligning its activities to those of other relevant EU agencies" (for example ENISA, the European Police College (CEPOL), Eurojust)<sup>191</sup>.

In particular, it stepped up its efforts to combat child pornography. The same requirements were emphasised by the European Agenda on Security, which was the natural extension of Commission President Jean-Juncker's political will to combat terrorism. The debate on European security demonstrated the high level of integration that had been achieved, since better implementation of the EU's legal instruments was a matter of closer dialogue between agencies and between sectors that had not previously been able to interact, such as justice and home affairs. Indeed, the experts stressed that the division of tasks between civil protection, military defence and police is one of the main challenges for the EU<sup>192</sup>.

Furthermore, there was an attempt to "bring together all internal and external dimensions of security", since "EU internal security and global security are mutually dependent and interlinked"<sup>193</sup>.

Until here, "the Cybersecurity Strategy can be seen as a continuation of the internal and external policies that have been developed by the EU in the area of NIS – and in the framework

---

Strategy of the European Union: An Open, Safe and Secure Cyberspace', 5.

<sup>190</sup> European Commission, 9.

<sup>191</sup> Christou, 'The Collective Securitisation of Cyberspace in the European Union', 22. In the words of Cecilia Malmström, European Commissioner for Home Affairs: "We can't let cybercriminals disrupt our digital lives. A European Cybercrime Centre within Europol will become a hub for cooperation in defending an internet that is free, open and safe" European Commission, 'An EU Cybercrime Centre to Fight Online Criminals and Protect E-Consumers', 28 March 2012, 1, [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_12\\_317](https://ec.europa.eu/commission/presscorner/detail/en/IP_12_317). (European Commission, 2012, p. 1) A fundamental component of the EC3 is the Joint Cybercrime Action Taskforce (J-CAT), which has been able to carry out crucial operations using both public and private resources. The "J-CAT is subject to a very specific legal framework that allows it to be flexible and to provide rapid responses by circumventing common bureaucratic and legal obstacles" See Christou, 'The Collective Securitisation of Cyberspace in the European Union', 23.

<sup>192</sup> Düll, Schoch, and Straub, 'Cybersecurity in the European Union', 4. "The main challenges within the EU are the division of tasks between civil defence, military defence and police, the defence against cyberattacks on critical infrastructures, the quantitative detection of security threats and how deep state security measures can interfere with individual freedom".

<sup>193</sup> European Commission, 'COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS The European Agenda on Security', 28 April 2015, 4, COM(2015) 185 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52015DC0185>.

of the EU–US Working Group on Cyber-Security and Cyber-Crime (WGCC)”<sup>194</sup>.

While the previous themes were to some extent a continuation of previous efforts, the strategy also heralded the beginning of a transformation of cybersecurity efforts, which had previously focused solely on the internal sphere.

"Cybersecurity efforts in the EU also involve the cyber defence dimension": "cybersecurity and cyberdefence were inextricably intertwined"<sup>195</sup>.

This simple affirmation had opened the way for civil and military approaches to co-operate in protecting Cyber Assets. Not only did the development of cyber defence capabilities require the creation of the right conditions to attract investment in both infrastructure and skills, but a whole cyber defence policy framework was needed for CSDP missions and operations. Therefore, the Strategy can be seen as a continuation of the European Union's commitment to the "progressive framing of a common Union defence policy", initiated by the Lisbon Treaty<sup>196</sup>.

---

<sup>194</sup> Ramses A. Wessel, 'Cybersecurity in the European Union: Resilience through Isolation?', in *The Routledge Handbook of European Security Law and Policy*, by Zhaklin V. Yaneva and Marzia Scopelliti, ed. E. Conde, 1st ed. (London ; New York: Taylor and Francis, 2019), 286, <https://doi.org/10.4324/9780429465918-18>.

<sup>195</sup> Renda, 'THE DEVELOPMENT OF EU CYBERSECURITY POLICY: FROM A COORDINATING ACTOR TO A CYBER POWER?', 478.

<sup>196</sup> Elena Suzana and Izabela Cristina Bacian, 'Implementation of the Lisbon Treaty Provisions on the Common Security and Defence Policy (CSDP)', Briefing (European Parliamentary Research Service, February 2016), 1, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/573285/EPRS\\_BRI\(2016\)573285\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/573285/EPRS_BRI(2016)573285_EN.pdf). The Treaty of Lisbon introduced a flexible framework for the development of the CSDP, which it is useful to outline here. Its main components are the mutual assistance clause (Article 42(7) TEU), permanent structured cooperation (Articles 42(6) and 46 TEU and Protocol No 10), enhanced cooperation (Article 20 TEU) and the possibility to entrust CSDP operations to a group of Member States (Article 44 TEU).

The mutual assistance clause is somehow reminiscent of Article 5 of the NATO treaty because it compels mutual military assistance in the event of an attack. "If a Member State is the victim of armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with Article 51 of the United Nations Charter. This shall not prejudice the specific character of the security and defence policy of certain Member States". This instrument was invoked for the first time by France in 2015, immediately after the terrorist attack in Paris, confirming the possibility of activating it against terrorism provided for by the European Parliament in 2012. Although it demonstrated its flexibility, its lack of procedural precision remains reprehensible.

The solidarity clause was introduced to enable a joint European response in the event of a terrorist attack or a natural or man-made disaster affecting a Member State. "The Union and its Member States shall act jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster. The procedure underlying solidarity has been established by a decision of the EU Council in accordance with Article 222 TFEU. See Council of the European Union, '2014/415/EU: Council Decision of 24 June 2014 on the Arrangements for the Implementation by the Union of the Solidarity Clause', 192 OJ L § (2014), <http://data.europa.eu/eli/dec/2014/415/oj/eng>.

Permanent Structured Cooperation is a mechanism that allows Member States to enhance their cooperation in the framework of the CFSP. "Those Member States whose military capabilities fulfil higher criteria and which have made more binding commitments to one another in this area with a view to the most demanding missions shall establish permanent structured cooperation within the Union framework. [...]". In this way, the "permanent structured cooperation acts as an 'umbrella for smaller packages of flexible cooperation'". See Suzana and Bacian, 'Implementation of the Lisbon Treaty Provisions on the Common Security and Defence Policy (CSDP)', 3. A political agreement on PESCO was reached in 2017 and consolidated by an EU Council decision. See Council of the European Union, 'Council Decision (CFSP) 2017/2315 of 11 December 2017 Establishing Permanent Structured Cooperation (PESCO) and Determining the List of Participating Member States', 331 OJ L § (2017), <http://data.europa.eu/eli/dec/2017/2315/oj/eng>.

In the wake of these interventions, “the Strategy also, for the first time, includ[ed] specific action points for cyber-defence under the aegis of the CFSP”<sup>197</sup>.

However, it is clear that the Communication was not the only vehicle for efforts in this area, which were pursued through a synergetic set of policies. For example, at the end of the same year, the European Council held the first thematic debate on defence since the entry into force of the Lisbon Treaty<sup>198</sup>. The context was one of constrained defence budgets in a fragmented European defence market, in which Member States had to take greater responsibility to keep pace and develop in complementarity with NATO and other international partners. Priorities included increasing the impact of CSDP policies by exploiting external partnerships, but in particular working to develop the EU's rapid response capabilities. Responsiveness required a stable framework of rules, which could benefit from synergies between CSDP and other justice actors, certainly involved in horizontal issues such as illegal migration, organised crime and terrorism.

But effectiveness was not only a question of speed, as it was also influenced by the diversity of technological capabilities available. With regard to cyber capabilities, a roadmap of projects involving training and exercises was being developed to improve the protection of assets, in line with the EU's cyber security strategy.

The creation of an “integrated, sustainable, innovative and competitive European Defence Technological and Industrial Base (EDTIB)” would have encouraged these activities through intelligent funding of dual-use research projects and appropriate certifications to maximise assessments and interoperability<sup>199</sup>.

All these activities had in common an inherent transparency and information sharing between partners, aspects that had been made possible by the new European Defence Agency Code of Conduct on Pooling and Sharing<sup>200</sup>.

All military domains could thus benefit from the dynamism that has always characterised the European common market, not only the traditional ones. “Cyberspace is often described as the fifth domain of military activity, equally critical to European Union (EU) Common Security and Defence Policy (CSDP) implementation as the domains of land, sea, air, and

---

That said about PESCO, the enhance cooperation can be described as a similar mechanism, but that can be applied to any policy area belonging to the Union's non-exclusive competencies.

Finally, the possibility to entrust CSDP operations to a group of Member States is a mechanism to “be tailor-made for CSDP missions and operations, allowing for a more timely and rapid response to crises”. See Suzana and Bacian, ‘Implementation of the Lisbon Treaty Provisions on the Common Security and Defence Policy (CSDP)’, 4.

<sup>197</sup> Dewar, ‘Cyber-Lisbon?’, 15.

<sup>198</sup> Council of the European Union, ‘European Council 19/20 December 2013 Conclusions’, 20 December 2013, 1, EUCO 217/13, [https://www.consilium.europa.eu/uedocs/cms\\_data/docs/pressdata/en/ec/140245.pdf](https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/140245.pdf).

<sup>199</sup> Council of the European Union, ‘Common Security and Defence Policy’, 19 December 2013, 1–11, [https://www.consilium.europa.eu/uedocs/cms\\_data/docs/pressdata/en/ec/140214.pdf](https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/140214.pdf).

<sup>200</sup> ““Pooling & Sharing” is a EU concept which refers to Member States-led initiatives and projects to increase collaboration on military capabilities. The pooling of capabilities occurs when several Member States decide to use capabilities either nationally owned or multi-nationally procured - on a collective basis. Sharing or more precisely role-sharing is when some Member States relinquish some capabilities with the assumption or the guarantee that other countries will make them available when necessary.” See European Defence Agency, ‘EDA’s Pooling & Sharing’, 30 January 2013, 1, [https://eda.europa.eu/docs/default-source/eda-factsheets/final-p-s\\_30012013\\_factsheet\\_cs5\\_gris](https://eda.europa.eu/docs/default-source/eda-factsheets/final-p-s_30012013_factsheet_cs5_gris).

space”<sup>201</sup>. Following urgent calls for a specific EU Cyber Defence Policy Framework in 2013, the EU Council stepped in to identify a number of priority areas, some of which reflected needs arising from general security and defence policy. Just as the development of military capabilities was necessary, so too was the development of specific cyber capabilities for missions.

The aim was to create the conditions for enhanced cooperation between Member States, to find common requirements for a minimum level of security to ensure mutual recognition, and to facilitate the exchange of cyber intelligence through improved cooperation between national military CERTs. In addition, the same minimum requirements had to be applied to the External Action Service in order to ensure its secure functioning.

Another not insignificant aspect was the creation of standards for training, both to standardise and to ensure the availability of useful skills in a sector of such high specificity<sup>202</sup>.

This was and still is a necessary precondition for the development of effective partnerships, both horizontally, with the private sector, and vertically, with European institutions and international partners, as also enshrined in the joint declaration of the European Council and NATO<sup>203</sup>.

As cyberspace is a rapidly evolving domain, the development of cyber capabilities would have ensured the possibility of synergies not only in the military but also in other policy areas.

This would have made it possible to achieve strategic autonomy through skilful policy integration, as advocated by then-High Representative of the Union for Foreign Affairs and Security Policy Federica Mogherini. This was precisely the aim of the Global Strategy for European Foreign and Security Policy (EUGS), where the word “Global” is not just intended in a geographical sense: it also refers to the wide array of policies and instruments the Strategy promotes”<sup>204</sup>.

In this context, the “EUGS elevated the status of cybersecurity by integrating it into the EU’s grand strategy”, aiming to enhance “effectiveness in different domains of which cyberspace has given particular attention”<sup>205</sup>.

While Europe was striving for a strong UN as the bedrock of the multilateral rules-based order, cybersecurity was enumerated among the priorities for the external action, as an essential component both of the international scenario, and of EU as a security community. Therefore, the European Union’s plan was to assist “Member States in protecting themselves against cyber threats while maintaining an open, free and safe cyberspace”<sup>206</sup>.

---

<sup>201</sup> Council of the European Union, ‘EU Cyber Defence Policy Framework’, 18 November 2014, 2, <https://ccdcoe.org/uploads/2018/11/EU-141118-EUCyberDefencePolicyFrame-2.pdf>.

<sup>202</sup> Council of the European Union, 11.

<sup>203</sup> Council of the European Union and NATO, ‘Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization’, 8 July 2016, <https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf>.

<sup>204</sup> Council of the European Union, ‘Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union’s Foreign and Security Policy’, June 2016, 4, [https://www.eeas.europa.eu/sites/default/files/eugs\\_review\\_web\\_0.pdf](https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf).

<sup>205</sup> Renda, ‘THE DEVELOPMENT OF EU CYBERSECURITY POLICY: FROM A COORDINATING ACTOR TO A CYBER POWER?’, 470.

<sup>206</sup> Council of the European Union, ‘Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union’s Foreign and Security Policy’, 21.



Hence the importance of the concept of resilience, which is translated from internal action to the Union's external action, both with regard to NATO and third countries<sup>207</sup>.

The assistance was focused on improving the resilience of critical infrastructures and telecom infrastructures, and reducing cybercrime. That “requir[ed] weaving cyber issues across all policy areas, reinforcing the cyber elements in CSDP missions and operations, and further developing platforms for cooperation”<sup>208</sup>.

The hoped result was the creation of a common cyber security culture to be complemented by a strong and coherent external action, which was a “combination of external and internal security policies [... in a] comprehensive approach”<sup>209</sup>.

The same necessity to effectively respond to cyber-attacks was stressed by the then-President of the European Commission Jean-Claude Juncker in its state of the Union speech, which underlined how “Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks. [...] Cyber-attacks know no borders and no one is immune”<sup>210</sup>.

While the Global Strategy had identified a number of priority areas where the Union needed to develop common approaches, the European Council had drawn attention to the need to develop a European defence industrial base in order to increase its strategic autonomy<sup>211</sup>.

Although investment in defence and the development of new military capabilities will always remain the responsibility of the Member States, the Union's policies could help to improve the defence industry by making it more competitive in the common market, stimulating cooperation and reducing unnecessary duplication. Following the adoption of the first two defence directives<sup>212</sup> the Commission proposed an action plan specifically focused

---

<sup>207</sup> Wessel, ‘Cybersecurity in the European Union: Resilience through Isolation?’, 285.

<sup>208</sup> Council of the European Union, ‘Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union’s Foreign and Security Policy’, 22. The main proposals for concrete EU external action can be summarised in five main points. First, a better and shared assessment of internal and external threats through shared intelligence, investment in satellite and UAV surveillance, and the introduction of data retention of passenger name records. Second, new investment in digital capabilities to secure data, networks and critical infrastructure in the European digital space. Third, defence cooperation must become the norm under the coordination of the EDA (European Defence Agency), while Member States retain sovereignty in their defence decisions. A strong role for the European External Action Service is needed to complement the work of other EU institutions. Fourthly, cooperation between Member States must be comprehensive in both military and civilian missions, including strengthening cooperation between law enforcement, judicial and intelligence services. Fifth, European diplomacy must be responsive and fully grounded in the Lisbon Treaty.

<sup>209</sup> Renda, ‘THE DEVELOPMENT OF EU CYBERSECURITY POLICY: FROM A COORDINATING ACTOR TO A CYBER POWER?’, 470.

<sup>210</sup> Jean-Claude Juncker, ‘Speech by President Jean-Claude Juncker - State of the Union Address 2017’, 13 September 2017, [https://ec.europa.eu/commission/presscorner/api/files/document/print/en/speech\\_17\\_3165/SPEECH\\_17\\_3165\\_EN.pdf](https://ec.europa.eu/commission/presscorner/api/files/document/print/en/speech_17_3165/SPEECH_17_3165_EN.pdf).

<sup>211</sup> European Commission, ‘Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - European Defence Action Plan’, 30 November 2016, COM/2016/0950 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016DC0950>.

<sup>212</sup> European Parliament and Council of the European Union, ‘Directive 2009/43/EC of the European Parliament and of the Council of 6 May 2009 Simplifying Terms and Conditions of Transfers of Defence-Related Products within the Community (Text with EEA Relevance)’, 146 OJ L § (2009),

on the single market<sup>213</sup>.

But, as already mentioned, the market is not an issue limited to European policies, and certainly not to defence alone. After this necessary parenthesis on the CSDP, it must be stressed that the development of research and a solid industrial base are also enabling conditions for cybersecurity. There is a risk that Europe will become too dependent not only on ICT produced elsewhere, but also on security solutions developed outside its borders.

“It [was] key to ensure that hardware and software components produced in the EU and in third countries that are used in critical services and infrastructure and increasingly in mobile devices are trustworthy, secure and guarantee the protection of personal data”<sup>214</sup>.

To achieve this goal, all actors in the cybersecurity supply chain needed to prioritise cybersecurity, implement appropriate risk management and adopt security standards and solutions. Therefore, the right incentives need to be put in place, both in terms of obligations and legal instruments. For these reasons, the Commission hoped for the rapid adoption of the proposed NIS Directive, whose obligations represent the first solid attempt at harmonisation in Europe. At the same time, the identification of security standards under the umbrella of EU voluntary certification schemes was another key component.

These initiatives underline the close relationship between the market and Europe's digitalisation policy, which President Juncker himself identified as a priority at the start of his mandate: “I believe that we must make much better use of the great opportunities offered by digital technologies, which know no borders. To do so, we will need to have the courage to break down national silos in telecoms regulation, in copyright and data protection legislation, in the management of radio waves and in the application of competition law”<sup>215</sup>.

This broad understanding of the Union's market competence has been an important pillar in widening the scope of the Euro-Union's action. “The EU refers to an obvious economic element, which relates to the completion of the DSM: citizens need trust and confidence to engage in new connected technologies and to use e-commerce facilities”. This method “provid[ed] some hooks for cybersecurity measures related to the functioning of the free

---

<http://data.europa.eu/eli/dir/2009/43/oj/eng>; European Parliament and Council of the European Union, ‘Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the Coordination of Procedures for the Award of Certain Works Contracts, Supply Contracts and Service Contracts by Contracting Authorities or Entities in the Fields of Defence and Security, and Amending Directives 2004/17/EC and 2004/18/EC (Text with EEA Relevance)’, 216 OJ L 5 (2009), <http://data.europa.eu/eli/dir/2009/81/oj/eng>.

<sup>213</sup> European Commission, ‘European Defence Action Plan’, 5. There were three main measures. Firstly, the creation of a European Defence Fund (EDF) to support defence research in innovative technologies, products and services and to ensure the competitiveness of the defence sector. Second, to stimulate investment in the supply chain and ensure market access for innovative companies, especially SMEs. Thirdly, to strengthen the defence market through openness and competition, building on the existing framework of EU directives.

<sup>214</sup> European Commission, ‘JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace’, 12.

<sup>215</sup> Jean-Claude Juncker, ‘A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change - Political Guidelines for the next European Commission’, 15 July 2014, 6, [https://commission.europa.eu/system/files/2019-09/juncker-political-guidelines-speech\\_en.pdf](https://commission.europa.eu/system/files/2019-09/juncker-political-guidelines-speech_en.pdf). For further information about the Digital Single Market Strategy see European Commission, ‘COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - A Digital Single Market Strategy for Europe’, 6 May 2015, COM(2015) 192 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN>.

movement or competition rules”<sup>216</sup>, like for the just mentioned NIS directive, since “security of network and information systems is seen as essential for the functioning of the internal market”<sup>217</sup>.

But many other interventions can be traced back to this area of competence. Examples include the eIDAS regulation on digital identity and trust services, or the so-called Cybersecurity Act, which renewed ENISA's mandate and laid the foundations for a European cybersecurity certification scheme to ensure trust and mutual recognition of products and services. In fact, “the lack of interoperable solutions (technical standards), practices (process standards) and EU-wide mechanisms of certification [were] among other gaps affecting the single market in cybersecurity. In this context, cybersecurity was identified as one of the ICT Standardisation Priorities for the Digital Single Market”<sup>218</sup>.

The regulation would have helped to overcome some of the inherent problems of the early years of the digital market. Firstly, it would have helped to foster the emergence of extended cross-sectoral cooperation mechanisms for incident response. Cybersecurity cannot be approached in watertight compartments, but requires a comprehensive response that can take into account its horizontal nature. Secondly, it would address the still high fragmentation that characterises the Digital Single Market with regard to cybersecurity products and services, thus promoting a more homogeneous development of the sector. In this context, certification would also have promoted the creation of a stable cybersecurity industry<sup>219</sup>.

In a society that was moving from the connection of specific devices to ubiquitous connectivity, the mid-term assessment of the Digital Single Market Strategy had already made it possible to assess the benefits in terms of cybersecurity policy by creating a European ICT framework and a minimum set of rules for responding to attacks and incidents<sup>220</sup>.

The final aspect of the strategy concerns the EU's international posture, particularly in responding to cyber-attacks. “In its international cyberspace policy, the EU will seek to promote openness and freedom of the Internet, encourage efforts to develop norms of behaviour and apply existing international laws in cyberspace”. In fact, “the EU [did] not call for the creation of new international legal instruments for cyber issues”, but simply wanted to ensure the enforcement of existing instruments in cyberspace<sup>221</sup>, and help third countries

---

<sup>216</sup> Wessel, ‘Cybersecurity in the European Union: Resilience through Isolation?’, 288.

<sup>217</sup> Wessel, 289. The NIS directive will be further analysed in paragraph III.2.1.

<sup>218</sup> European Commission, ‘COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry’, 5 July 2016, 8, COM/2016/0410 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0410>.

<sup>219</sup> European Commission, 3.

<sup>220</sup> European Commission, ‘COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the Mid-Term Review on the Implementation of the Digital Single Market Strategy A Connected Digital Single Market for All’, 10 May 2017, 12, COM/2017/0228 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017DC0228>. Other notable achievements include the reform of electronic communications with the introduction of the European Code, the implementation of 5G, the introduction of the General Data Regulation and the proposal for the reform of privacy in electronic communications and other measures on the circulation of non-personal data, and the fight against illegal content on large platforms.

<sup>221</sup> European Commission, ‘JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - Cybersecurity

improve the protection of their critical information infrastructures.

Awareness of the risks posed by cyberspace led the Council of the European Union to adopt conclusions on cyber diplomacy and then a first draft of a code of conduct to be adopted in response to a cyber-attack. “The EU stress[ed] that clearly signalling the likely consequences of a joint EU diplomatic response to such malicious cyber activities influences the behaviour of potential aggressors in cyberspace thus reinforcing the security of the EU and its Member States”<sup>222</sup>.

Although the problem of correctly attributing cyber-attacks remains unresolved<sup>223</sup>, many responses can be made even in the absence of precise identification of the perpetrators. This would have made it possible to establish an appropriate level of coordination at national and European level, while maintaining dialogue with international partners.

### II.3.3 The update of the strategy

Although “the Cybersecurity Strategy and its holistic approach demonstrate the best that the changes brought in by the Treaty of Lisbon has to offer, it is not complete”<sup>224</sup> because some ontological weaknesses remained, particularly the lack of EU competences in the CFSP. “While the EU sought to establish itself as an actor in the international sphere [...]”, the reality was that “its scope as an actor – what it can actually do – [was] much more limited in this area [...], when compared to criminal justice matters or the resilience of the internal market”<sup>225</sup>.

The evaluation of the strategy published by the European Commission in 2017 confirmed that all its objectives were still relevant, but that the technological scenario had changed drastically, with the emergence of new technologies, a further increase in cybercrime and new threat actors.

In terms of effectiveness, the strategy appears to have only partially achieved its objectives, partly due to its very vague formulation. The pursuit of cyber resilience is a perfect example of this vagueness. The adoption of the NIS Directive had certainly helped, but the EU's cyber capabilities for responding to large-scale incidents were still rather limited. Cooperation between Member States was still voluntary, while cooperation with the private sector was still patchy. The same was true of relations between European institutions, which were based on informal agreements.

The goal of reducing cybercrime was a complete failure, perhaps because it was too ambitious. Despite the efforts of the EC3 at Europol, which certainly facilitated cooperation between Member States, the resources available were rather limited. The main challenges were on the procedural side of criminal investigations.

In contrast, little progress had been made towards a single market for cybersecurity products, which remained highly fragmented. Efforts to create a European certification scheme were thwarted by the proliferation of similar national initiatives aimed at defending

---

Strategy of the European Union: An Open, Safe and Secure Cyberspace’, 15.

<sup>222</sup> Council of the European Union, ‘Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (“Cyber Diplomacy Toolbox”)', 7 June 2017, 5, 9916/17, <https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf>.

<sup>223</sup> To illustrate the complexity of the issue and the need to arrive at a procedure that allows for a rapid response, the example of Stuxnet attribution can be recalled. See Düll, Schoch, and Straub, ‘Cybersecurity in the European Union’, 6.

<sup>224</sup> Dewar, ‘Cyber-Lisbon?’, 16.

<sup>225</sup> Dewar, 16.

national interests.

Consistently, also in the field of defence, the involvement of the Member States remained rather low in spite of many initiatives.

The only unmitigated success was the international convergence on cyber diplomacy practices, demonstrating EU's weight as a legislator at the international level. "The EU has been able to present a coherent approach on major global cyber debates, with a convergence of Member States' positions on different cyber diplomacy issues"<sup>226</sup>.

Both the rapid evolution of the digital scenario and the inadequacy of the first strategy led to an update of the plans and a new cybersecurity strategy was presented by the European Commission in 2017.

"Cybersecurity is critical to both our prosperity and our security. [...] Malicious cyber activities not only threaten our economies and the drive to the Digital Single Market, but also the very functioning of our democracies, our freedoms and our values. Our future security depends on transforming our ability to protect the EU against cyber threats: both civilian infrastructure and military capacity rely on secure digital systems"<sup>227</sup>.

This opened a sort of third phase, during which cybersecurity was finally deemed as a political priority<sup>228</sup>.

The Cybersecurity strategy in 2013 was an "high-level political document rather than a detailed and binding action plan"<sup>229</sup> but "the continuously evolving and deepening threat landscape call[ed] for more action to withstand and deter attacks"<sup>230</sup>.

"The strategy accentuated the shift from an interconnected world to a hyper-connected world with the introduction of the Internet of Things (IoT) devices"<sup>231</sup>.

From its very first pages, two considerations emerge that demonstrate the new awareness of the European Union as a player on the global stage. Firstly, the need for a choral response from all actors directly or indirectly involved in cybersecurity. No less important is the recognition of cyberspace as a new domain of conflict.

Influenced by the aforementioned global strategy, "the strategy took geopolitical shifts in international politics into consideration and acknowledged that geopolitical rivalry continues in cyberspace"<sup>232</sup>.

Kinetic attacks or the direct use of force are no longer the only means of achieving national goals. Cyber tools can also be used to achieve these goals, and they can also interfere with democratic processes.

---

<sup>226</sup> European Commission, 'Commission Staff Working Document - Assessment of the EU 2013 Cybersecurity Strategy', 13 September 2017, 57–60, SWD(2017) 295 final, [https://ec.europa.eu/transparency/documents-register/api/files/SWD\(2017\)295\\_0/de00000000176037?rendition=false](https://ec.europa.eu/transparency/documents-register/api/files/SWD(2017)295_0/de00000000176037?rendition=false).

<sup>227</sup> European Commission, 'JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU', 13 September 2017, 2, JOIN 450, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017JC0450>.

<sup>228</sup> Timmers, 'The European Union's Cybersecurity Industrial Policy'.

<sup>229</sup> Timmers, 369.

<sup>230</sup> European Commission, 'JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU', 3.

<sup>231</sup> Renda, 'THE DEVELOPMENT OF EU CYBERSECURITY POLICY: FROM A COORDINATING ACTOR TO A CYBER POWER?', 483.

<sup>232</sup> Renda, 483.

“The EU is well placed to address cybersecurity, given the scope of its policies and the tools, structures and capabilities at its disposal. While Member States remain responsible for national security, the scale and cross-border nature of the threat make a powerful case for EU action providing incentives and support for Member States to develop and maintain more and better national cybersecurity capabilities, while at the same time building EU-level capacity”.<sup>233</sup>

The division follows the three main policy lines now established in the Union's work, already defined in the previous strategy, in line with the historical division of competences into pillars. On the basis of this order of content, here is an attempt to highlight the main new features that were introduced in 2017.

The main area of intervention is that of resilience. A comprehensive approach to the issue is maintained, with the intention of adopting multi-sectoral policies.

While the introduction of the NIS Directive ideally represented the first milestone for European cybersecurity, the implementation of which had to be accelerated and extended, the Commission developed some lines of action to complement this framework. One of the limitations of the regulatory framework was the problem of information exchange, which faced a number of obstacles on the part of both private and public bodies. “Governments and public authorities are reluctant to share cybersecurity-relevant information for fear of compromising national security or competitiveness”<sup>234</sup>.

This is a natural consequence of the exclusion of public administration from the scope of the Regulation, which was in fact intended to be extended<sup>235</sup>. It is therefore proposed to invest in the development of Information Sharing and Analysis Centres (ISACs) to facilitate the exchange of information in the different production sectors.

Improving the flow of information was linked to the desire to improve the European Rapid Response Mechanism for emergencies by integrating cybersecurity aspects.

To this end, the European Commission had prepared a project to explain how Member States could benefit from existing crisis management mechanisms at European level to manage crises directly or indirectly related to the cyber domain by implementing the necessary operational rules<sup>236</sup>.

---

<sup>233</sup> European Commission, ‘JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU’, 3.

<sup>234</sup> European Commission, 7.

<sup>235</sup> This is one of the changes that would characterise the structure of the new NIS. The issue of reform is discussed in paragraph III.2.2.

<sup>236</sup> The European Union has now established two levels of crisis response.

The first policy is rooted in the first EU Emergency and Crisis Coordination Arrangements (CCA), dating back to 2005, the development of which was linked to the introduction of the solidarity clause. Following this development, the Council of the European Union introduced a procedure for the implementation of solidarity in parallel with the replacement of the EAC by the EU Integrated Political Crisis Response arrangements (IPCR). The latter has recently been officially institutionalised by a Council implementing decision. CITE Council 2018 For further information see Iñigo de Miguel Beriain, Elena Atienza-Macías, and Emilio Armaza Armaza, ‘The European Union Integrated Political Crisis Response Arrangements: Improving the European Union’s Major Crisis Response Coordination Capacities’, *Disaster Medicine and Public Health Preparedness* 9, no. 3 (June 2015): 234–38, <https://doi.org/10.1017/dmp.2015.10>. Also at the political level is the External Crisis Response System, which is activated following events affecting the external dimension of the European Union.

The second level of response is the operational exchange of information at European level, using the information infrastructure and platforms of the European Commission. Reference has already been made to the

The other measures related to resilience are nothing more than the implementation of a long-announced change. In fact, the issue of stabilising ENISA's mandate has been discussed for a long time, but has always been postponed by successive extensions. The same can be said of the issue of certification of cyber products and services, which was raised in the previous strategy, which launched a study phase to find the most effective solution. The opportunity to address both issues was provided by the proposed Regulation for a Cybersecurity Act, presented by the Commission on the same day as the strategy update<sup>237</sup>.

This approach would also have helped to create a real market for cyber solutions by introducing the principle of security by design into the ICT sector, so that vulnerabilities are addressed before they are marketed. More attention needs to be paid to producer liability, especially in view of the interconnectedness of digital products.

The sensitivity of the issue is also underlined by the Commission's intention to introduce a specific framework for reviewing foreign investment in the EU for the acquisition of critical technologies, which should certainly include cybersecurity. The free movement of goods within the Union must be accompanied by greater restrictions on the export of technological solutions that are crucial to European competitiveness. In this respect, it is normal to consider cybersecurity as a minimum criterion for market access.

According to some commentators, after these interventions, it is finally possible to say that “the general industrial policy of 2017 fully acknowledged the ongoing development of cybersecurity industrial policy measures. [...] EU cybersecurity industrial policy is thus firmly embedded in general EU industrial policy”<sup>238</sup>.

In contrast to the first strategy, the EU had put in place a concrete set of policies capable of intervening in market risks. “For the first time the risk was signalled that cyber industry and talent might not stay in Europe given that it were mainly non-European investors that engaged in acquisitions of the relatively small European cybersecurity companies [...]. The need that the EU retains and develops the essential capacities to secure its digital economy, society and democracy”<sup>239</sup> had led to a shift from a reactive to a proactive approach to protect European prosperity, society and values, as well as fundamental rights and freedoms.

This is proof that, for the first time, the Union's strategic autonomy had become a fundamental element of its action and regulation.

It should be noted that the maintenance and development of capabilities implies the prior development of security capabilities. While this has so far been achieved through public-private partnerships, the Commission had proposed to “reinforce EU cybersecurity capability through a network of cybersecurity competence centres”<sup>240</sup>, coordinated by a European

---

ARGUS rapid alert system. See footnote 136. For further information see European Commission, ‘Commission Recommendation (EU) 2017/1584 of 13 September 2017 on Coordinated Response to Large-Scale Cybersecurity Incidents and Crises’, *OJ L*, 13 September 2017, <http://data.europa.eu/eli/reco/2017/1584/oj/eng..>

<sup>237</sup> European Commission, ‘Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the “EU Cybersecurity Agency”, and Repealing Regulation (EU) 526/2013, and on Information and Communication Technology Cybersecurity Certification (“Cybersecurity Act”)', 2017/0225 (COD) § (2017), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0477>.

<sup>238</sup> Timmers, ‘The European Union’s Cybersecurity Industrial Policy’, 369.

<sup>239</sup> Timmers, 370.

<sup>240</sup> European Commission, ‘JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU’, 9.

Cybersecurity Research and Competence Centre.

In its first phase, this new institution should have a role in coordinating research efforts, supporting testing activities to ensure effective adoption of cybersecurity certification, and developing new standards to support the creation of new sector expertise<sup>241</sup>.

At a more advanced stage of its work, however, its integration into the defence sector should be supported. “The Centre would need to work closely and in full complementarity with the European Defence Agency in the area of cyber defence, as well as with ENISA in the area of cyber resilience”<sup>242</sup>.

The second area of intervention is cybercrime, accompanied by the notion of deterrence. Significantly, the European framework aims to achieve effectiveness. “Effective deterrence means putting in place a framework of measures that are both credible and dissuasive for would-be cyber criminals and attackers. [...] Cyber-attacks should be promptly investigated and perpetrators brought to justice, or action taken to allow an appropriate political or diplomatic response”<sup>243</sup>.

Although Europol's Cybercrime Unit has played a central role in supporting Member States' investigations since its establishment, there has unfortunately been a widespread lack of investigative capacity to find useful information and digital traces. As a result, by 2017 it was clear that the problem was no longer a lack of substantive rules to prosecute crimes, but rather a lack of adequate technical capabilities. The Commission had already intervened by proposing several harmonisation measures in the first Cyber Strategy and new rules were about to be implemented. On the substantive side, there is the replacement of the directive on fraud and counterfeiting of non-cash means of payment, and on the procedural side the regulation facilitating cross-border access to electronic evidence<sup>244</sup>.

Therefore, Europol should become a reference point regarding the harmonisation of digital forensics and the latest network protocols should be adopted in the Union<sup>245</sup>.

It was precisely the improvement of the technological base that demonstrated the strong expansion of the common defence area. Member States, especially the more advanced ones, were invited to invest in the development of dual-use products and to make use of the

---

<sup>241</sup> European Commission, 9.

<sup>242</sup> European Commission, 10.

<sup>243</sup> European Commission, 12–13.

<sup>244</sup> ‘Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Combating Fraud and Counterfeiting of Non-Cash Means of Payment and Replacing Council Framework Decision 2001/413/JHA’ (2017), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52017PC0489>; ‘Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for Electronic Evidence in Criminal Matters’ (2018), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:225:FIN>.

<sup>245</sup> The European Commission was actively promoting the adoption of IPv6 to improve identification in cybercrime investigations. IPv6, the next generation Internet Protocol, expands the address space available to devices connected to the Internet. Unlike its predecessor, IPv4, which was limited by the number of unique addresses available, IPv6 provides a large pool of addresses. The number of unique addresses is virtually unlimited. This large address space allows a single IP address to be assigned to each user. This allows for more accurate identification during cybercrime investigations. With a unique IP address assigned to each user, law enforcement and cybersecurity professionals can more effectively trace and track individual online activities. This can help identify and investigate potential criminals. The European Commission's endorsement of IPv6 reflects its recognition of the potential benefits of IPv6 in improving identification capabilities and strengthening the overall effort to improve cyber security.



possibilities offered by PESCO<sup>246</sup>, which had just started its activities following its consolidation by the EU Council<sup>247</sup>. “Enhanced cooperation among member states for the development of cyber defence capabilities is of great importance for the EU’s cyber deterrence”<sup>248</sup>.

Given the momentous changes brought about by the introduction of the new European Data Protection Regulation, a new collaboration with the private sector was also required. “In the context of cybercrime, private undertakings need to be able to share information on concrete incidents with law enforcement – including personal data – in full respect of data protection rules”<sup>249</sup>.

The framework demonstrated the shift towards a proactive approach, both from an internal and market perspective and from an external defence perspective. The latter aspect has been strengthened not only by the launch of several European cooperation projects, also thanks to the coordination of the EDA<sup>250</sup>, but also by the introduction of a specific set of rules for managing the diplomatic response to cyber incidents. The package provides for “restrictive measures which can be used to strengthen the EU’s response to activities that harm its political, security and economic interests”<sup>251</sup>. This shows how they want to promote the application of international law and fundamental rights in cyberspace.

Although there was a change of approach on the part of the EU, as evidenced by the adoption of stronger measures for greater strategic weight, several shortcomings remained inherent in the regulatory framework. The multiplicity of interventions lacked coherence between different policies, and the fragmented nature of national interventions had not diminished. The right balance needed to be reached between intervention at national and European level. The main responsibility remained with the Member States, with Europe playing only a coordinating and secondary role.

Although the expansion of ENISA’s role has certainly had an impact on standardisation and cooperation, “the EU is still a long way from bundling all the measures in a single cybersecurity agency”<sup>252</sup>. “The questions and concerns touch the heart of the European project and are pushing cybersecurity up the political ladder”<sup>253</sup>. [This applies to the industrial development profile of cybersecurity, where] development it is also not likely to find a willing ear with

---

<sup>246</sup> European Commission, ‘JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU’, 17.

<sup>247</sup> See footnote 196. Among the various PESCO projects available online, the first joint efforts are worth mentioning: the Cyber Rapid Response Teams and Mutual Assistance in Cybersecurity and the Cyber Threats and Incident Response Information Sharing Platform.

<sup>248</sup> Renda, ‘THE DEVELOPMENT OF EU CYBERSECURITY POLICY: FROM A COORDINATING ACTOR TO A CYBER POWER?’, 484.

<sup>249</sup> European Commission, ‘JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU’, 16.

<sup>250</sup> The EDA began to play a central role in EU cybersecurity orchestration. The first project launched under its control was the Cyber Ranges Federation project, which aimed to bring together eleven national cyber ranges into an integrated system for real-time training and exercises in simulated operational environments. For further information, please visit ‘Eda’s Growing Role in Cybersecurity’, *European Defence Matters*, 2019.

<sup>251</sup> European Commission, ‘JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU’, 16.

<sup>252</sup> Düll, Schoch, and Straub, ‘Cybersecurity in the European Union’, 3.

<sup>253</sup> Timmers, ‘The European Union’s Cybersecurity Industrial Policy’, 379.

governments”<sup>254</sup>.

The same applies to the future of European defence. Despite the strengthening of cooperation between countries and the launch of joint projects, there is no real European Cyber Security Command<sup>255</sup>.

“Despite the EU’s prioritization of cyber defence, the EU lacking a centralized cyber command undermines its cyber defence capabilities”<sup>256</sup>. Without undermining the progress that has been achieved, a middle ground must surely be found.

#### II.3.4 The last EU cybersecurity strategy

Each strategy represents a snapshot of the context in which it was conceived. By juxtaposing the impressions captured by the strategies analysed, it is possible to highlight a crescendo punctuated by increasingly rapid technological progress. As if not to contradict Moore’s Law, the increase in computing power and the new possibilities opened up by digitalisation require decisive intervention. It is no coincidence that the strategy begins with the statement that “Cybersecurity is an integral part of Europeans’ security”<sup>257</sup>.

The knowledge that “cyberspace is increasingly exploited for political and ideological purposes”<sup>258</sup> creates a new set of threats that take advantage of the peculiar conformation of this new domain. Hybrid threats are now a constant, combining cyber-attacks and disinformation to target infrastructure and democratic processes<sup>259</sup>.

---

<sup>254</sup> Timmers, 379.

<sup>255</sup> As analysed above, a number of defence cooperation initiatives had undoubtedly already been launched, suffering from marked differences in threat perceptions and duplication of resources in the various Member States. In the same year, the Commission published a reflection paper on the future of European defence, in which three different scenarios of increasing integration were hypothesised. Each of these scenarios is not exhaustive, nor does it completely exclude the others.

The first hypothesis is that of largely voluntary cooperation, decided on a case-by-case basis in the face of each new emergency. The EU will play only a coordinating role.

The second hypothesis is that of a common defence, with increasing penetration of the European Union in financial and operational decisions, including the management of joint projects.

Finally, the third hypothesis is that of a common defence, based on the possibility expressed in Article 42 of the TEU, which calls for the progressive definition of a common defence policy. For further information see European Commission, ‘Reflection Paper on the Future of European Defence’, 7 June 2017, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017DC0315>.

<sup>256</sup> Renda, ‘THE DEVELOPMENT OF EU CYBERSECURITY POLICY: FROM A COORDINATING ACTOR TO A CYBER POWER?’, 482.

<sup>257</sup> European Commission, ‘JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - Report on Implementation of the EU’s Cybersecurity Strategy for the Digital Decade’, 23 June 2021, 1, JOIN 0166, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021JC0014>.

<sup>258</sup> European Commission, ‘JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - The EU’s Cybersecurity Strategy for the Digital Decade’, 16 December 2020, 2, JOIN 18, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020JC0018>.

<sup>259</sup> The problem, which had taken on a worrying dimension over the years, had prompted several interventions by the European institutions, starting with the Joint Framework on countering hybrid threats, immediately after the results of the US elections. See European Commission, ‘JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Joint Framework on Countering Hybrid Threats a European Union Response’, 6 April 2016, JOIN/2016/018 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018>. Following the chemical attack in Salisbury and the European Council’s request to the Commission to take action, a specific action plan on disinformation had been developed to create the tools to prevent possible interference during the 2019 European elections. In particular, the plan focuses on the willingness to exchange information, as demonstrated by the creation of an early warning system

Insecurity is the main obstacle to the use of online services and to digital citizenship, but the European Union lacks the necessary awareness of the threat scenario due to a lack of information cooperation between the public and private sectors and between the European institutions themselves, as highlighted in the previous strategy. This has serious implications for the ability to respond to a major cyber crisis.

Against the background of a growing threat, the new cybersecurity strategy is part of a general renewal of the entire European policy framework<sup>260</sup>. Its introduction is an integral part of shaping Europe's digital future, which is one of the priorities of the new von der Leyen Commission. The key points are to create its own strategic autonomy, reduce external dependencies and create the conditions for technology to serve citizens<sup>261</sup>.

This raises regulatory issues regarding the latest technological advances, such as artificial intelligence and 5G standards, in the context of a common market whose integration is being strengthened. Liability issues need to be addressed, both with regard to the behaviour of digital operators and the security of digital products. The more general issue of cybersecurity remains a cross-cutting one, divided into three priority areas, similar to the pillar structure.

In fact, the essential theme is resilience, which best represents the effort behind digital security. It is a constant race to create and implement patches after a new vulnerability is discovered.

Related to this, "EU rules on the security of Network and Information Systems (NIS) are at

---

against disinformation. See Council of the European Union. 'Council of the European Union, 'Rapid Alert System - Strengthening Coordinated and Joint Responses to Disinformation', March 2019, [https://www.eeas.europa.eu/sites/default/files/documents/ras\\_factsheet\\_march\\_2019\\_0.pdf](https://www.eeas.europa.eu/sites/default/files/documents/ras_factsheet_march_2019_0.pdf); European Commission, 'JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Action Plan against Disinformation', 5 December 2018, JOIN(2018) 36 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018JC0036&qid=1690703950858>. This tool was also used against disinformation campaigns against the COVID-19. In particular during the pandemic, ENISA also intervened with a specific report on foreign interference through disinformation. See 'Foreign Information Manipulation and Interference (FIMI) and Cybersecurity', Threat Landscape (European Union Agency for Cybersecurity, December 2022), <https://data.europa.eu/doi/10.2824/7501>. 'Foreign Information Manipulation and Interference (FIMI) and Cybersecurity'. Threat Landscape. European Union Agency for Cybersecurity, December 2022. [<https://data.europa.eu/doi/10.2824/7501>](<https://data.europa.eu/doi/10.2824/7501>).

<sup>260</sup> The new threat scenario for the EU was highlighted in the Union's new security strategy, which now puts cyber-attacks on the same level as terrorism and organised crime, and continues to move towards the goal of increased resilience. The need for a Joint Cyber Security Unit to improve the European mutual assistance mechanism in the event of a crisis was reiterated. At the same time, the achievements of the cyber diplomacy toolbox should serve as a basis for consolidating deterrence in cyberspace. See European Commission, 'Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy', 24 July 2020, COM/2020/605 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0605>.

<sup>261</sup> The European Commission had highlighted several priorities for action, which have been implemented. To briefly recall the main ones related to this discourse, one only has to think of the White Paper on Artificial Intelligence and the proposal for a Regulation on the regulation of AI, which has recently reached final adoption. This is accompanied by the allocation of important new resources for the uniform implementation of 5G communications security and the introduction of new rules on liability. In particular, the so-called Digital Services Act, which introduces new obligations for large platforms, has been approved. In terms of policies related to the smooth functioning of the market, the reform of the eIDAS regulation on digital identity and trust services, which introduces new standards for DLT systems, should also be mentioned. See

the core of the Single Market for cybersecurity”<sup>262</sup>.

For this reason, the Strategy builds on the work of its predecessor by focusing on the main shortcomings that need to be addressed through an appropriate amendment to the Directive. The most pressing problems were, on the one hand, the narrow scope, which did not reflect the real security architecture, leaving out key actors in the private sector, but above all the public administration as a whole. Linked to this, the uneven application also affected the possibility of effective cooperation and control by the competent authorities<sup>263</sup>.

It is also significant that the new NIS was presented at the same time as the critical infrastructure reform, whose legislation was still stalled in 2008. Both proposals were finally adopted in early 2023.

Another element that, together with the NIS reform, echoes previous shortcomings is the lack of information exchange between security actors. Efforts to promote the creation of ISACs and SOCs, which should be able to network at European level, are therefore reiterated. The ambitious goal is to create a cyber security shield capable of compensating for the lack of situational awareness by providing information to emergency response agencies<sup>264</sup>.

While in the past the discourse on resilience was always limited to critical infrastructure, which in itself does not necessarily involve digital issues, the recent debate has been permeated by a strong focus on more sophisticated technological solutions. Recalling the arguments on the need for strategic autonomy of the Union, technological research is certainly a factor of competitiveness. A number of examples can be cited in this respect, distinguishing between technologies at the service of institutions and technologies at the service of citizens. The first group certainly includes efforts to develop robust end-to-end encryption solutions<sup>265</sup> between institutions and agencies, as well as space communications.

The second group includes initiatives related to more traditional products, from 5G to the Internet of Things<sup>266</sup>. It is precisely in the field of telecommunications, given its ubiquitous and strategic nature, that the greatest efforts are being made. The Union has intervened with

---

<sup>262</sup> European Commission, ‘JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - The EU’s Cybersecurity Strategy for the Digital Decade’, 5.

<sup>263</sup> Renda, ‘THE DEVELOPMENT OF EU CYBERSECURITY POLICY: FROM A COORDINATING ACTOR TO A CYBER POWER?’, 486.

<sup>264</sup> Renda, 487.

<sup>265</sup> Quantum encryption, also known as quantum cryptography, is an advanced technique that uses the principles of quantum mechanics to secure communications. It uses individual particles of light, called photons, to transmit encryption keys between communicating parties. Unlike traditional methods, quantum encryption ensures the security of transmitted information by detecting any attempt at eavesdropping. It relies on fundamental properties of quantum mechanics, such as the uncertainty principle, to ensure the confidentiality and integrity of communication channels. By exploiting quantum mechanics, quantum encryption provides a highly secure approach to protecting sensitive information during transmission. For further information about the technical functioning see Zhang-Dong Ye et al., ‘Generic Security Analysis Framework for Quantum Secure Direct Communication’, *Frontiers of Physics* 16, no. 2 (28 December 2020): 21503, <https://doi.org/10.1007/s11467-020-1025-x>.

<sup>266</sup> Although it may appear to be of secondary importance, the European Internet infrastructure is one of the most important of the cutting-edge technologies mentioned. Consequently, the European Commission has highlighted the importance of preventing threats to the integrity and availability of the global DNS root system. Due to the variety of cyber-attacks made possible by the vulnerabilities of the DNS, the proposal for a public DNS instance was put forward. For the same reason of promoting the overall security of the Internet, the rapid adoption of the latest Internet standards, such as IPv6, is advocated. In fact, IPv6 was also supported by the previous strategy as a means of facilitating digital criminal investigations.

a specific package of policies to guide and standardise the actions of the Member States. Member States are instructed to fully implement 5G standards, mitigating shortcomings identified during the process<sup>267</sup>.

The attempt to minimise technological dependence on third countries is undeniable proof of the attention paid to strategic autonomy. “Whereas the principle of strategic autonomy already was embedded in the EU’s 2017 strategy in the 2020 strategy technological leadership and sovereignty have been prioritized”<sup>268</sup>.

Although the idea was still just a proposal, the Cybersecurity Industrial Technology and Research Competence Centre has already been appointed with the key role of developing technological sovereignty in cybersecurity, using all contributions from industry and academia.

The second central theme of the strategy is deterrence. Despite the similarities with previous work and the poor results achieved so far, some innovative features can be identified. The main aspect of maturity is the more precise understanding of the different actors involved in the response mechanism to a cybersecurity incident, which must be understood as a joint effort. In other words, whereas previously there was a greater focus on the individual components, there is now a greater awareness of the complexity and cross-sectoral nature of the individual contributions, which have been refined over time. For example, one can list NIS authorities, law enforcement and judicial authorities, external diplomatic authorities, and finally cyber defence. At the heart of this system, which plays an orchestrating role, is the Joint Cyber Security Unit. In addition to being a key building block for large-scale crisis response, it is also the instrument to consolidate the progress made both after the implementation of the Recommendation on a coordinated response to large-scale cybersecurity incidents and crises and the NIS Cooperation Group.

As requested by the Commission, its launch over the last few years has indeed helped to fill the gap left by the lack of a reliable reference point for the various European cybersecurity actors, where they could work together in a structured manner. It does not constitute a new body and does not centralise the competences of other authorities, but simply acts as a support by pooling the competences of different actors.

While there are no major updates in the fight against cybercrime, developments in the area of the Union's external action can be appreciated. Following the introduction of the Cybersecurity Toolbox in 2019 and its update in 2020<sup>269</sup>, there have already been several use

---

<sup>267</sup> Progress reports on the implementation of the Toolbox show an overall strengthening of communications security, although some States still have shortcomings. Most have adopted legislative measures to ensure that restrictions can be imposed, but others are still working on implementation. The risk of dependency on external providers therefore remains. There has been a marked improvement in technical requirements, which will certainly benefit from the recent implementation of NIS2 and the proposed Cyber Resilience Act. See NIS Cooperation Group, ‘Report on Member States’ Progress in Implementing the EU Toolbox on 5G Cybersecurity’ (NIS Cooperation Group, July 2020), [https://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=68510](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68510); NIS Cooperation Group, ‘Second Report on Member States’ Progress in Implementing the EU Toolbox on 5G Cybersecurity’ (NIS Cooperation Group, June 2023), <https://ec.europa.eu/newsroom/dae/redirection/document/96519>.

<sup>268</sup> Renda, ‘THE DEVELOPMENT OF EU CYBERSECURITY POLICY: FROM A COORDINATING ACTOR TO A CYBER POWER?’, 488.

<sup>269</sup> After the first draft of the Toolbox in 2017, its final adoption took place in 2019. It consists of a decision and a regulation of the Council of the European Union. Both were amended in 2020. Council of the European Union, ‘Council Regulation (EU) 2019/796 of 17 May 2019 Concerning Restrictive Measures against Cyber-

cases demonstrating the effectiveness of the European response.

The Union is also demonstrating its strength and ability to promote the principles of responsible behaviour in cyberspace: “The EU is best placed to advance, coordinate and consolidate Member States’ positions in international fora, and should develop an EU position on the application of international law in cyberspace”<sup>270</sup>.

On the other hand, much remains to be done on the military side, where it is hoped that the announced revision of the Cyber Defence Policy Framework will succeed in fostering greater cooperation between the different actors. Following the official recognition of cyberspace as a domain of operations in 2018 and the launch of the defence CERT network at the EDA, Member States will need to take full advantage of all the Union's support. For the moment, it seems possible to confirm that “the EU does not have a military doctrine and a military cyber command”, since “its main concern is law enforcement, crisis management, and international cooperation”<sup>271</sup>.

“The EU’s actorness concerning cybersecurity has evolved from mere economic and technical concerns to cybercrimes, technological leadership, strategic autonomy and international influence on third countries while the military dimension of EU cybersecurity policy has been lagging far behind its civilian and economic dimensions”<sup>272</sup>.

All the identified categories from the EU policies in this chapter are summarised in Figure 1. These are exploited to group the binding legislation that is presented in chapter III.

---

Attacks Threatening the Union or Its Member States’, 129I OJ L § (2019), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0796>; Council of the European Union, ‘Council Decision (CFSP) 2019/797 of 17 May 2019 Concerning Restrictive Measures against Cyber-Attacks Threatening the Union or Its Member States’, 129I OJ L § (2019), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019D0797>; Council of the European Union, ‘Council Implementing Regulation (EU) 2020/1125 of 30 July 2020 Implementing Regulation (EU) 2019/796 Concerning Restrictive Measures against Cyber-Attacks Threatening the Union or Its Member States’, 246 OJ L § (2020), [http://data.europa.eu/eli/reg\\_impl/2020/1125/oj/eng](http://data.europa.eu/eli/reg_impl/2020/1125/oj/eng); Council of the European Union, ‘Council Decision (CFSP) 2020/1127 of 30 July 2020 Amending Decision (CFSP) 2019/797 Concerning Restrictive Measures against Cyber-Attacks Threatening the Union or Its Member States’, 246 OJ L § (2020), <http://data.europa.eu/eli/dec/2020/1127/oj/eng>.

<sup>270</sup> European Commission, ‘JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - The EU’s Cybersecurity Strategy for the Digital Decade’, 20.

<sup>271</sup> Renda, ‘THE DEVELOPMENT OF EU CYBERSECURITY POLICY: FROM A COORDINATING ACTOR TO A CYBER POWER?’, 490.

<sup>272</sup> Renda, 490.

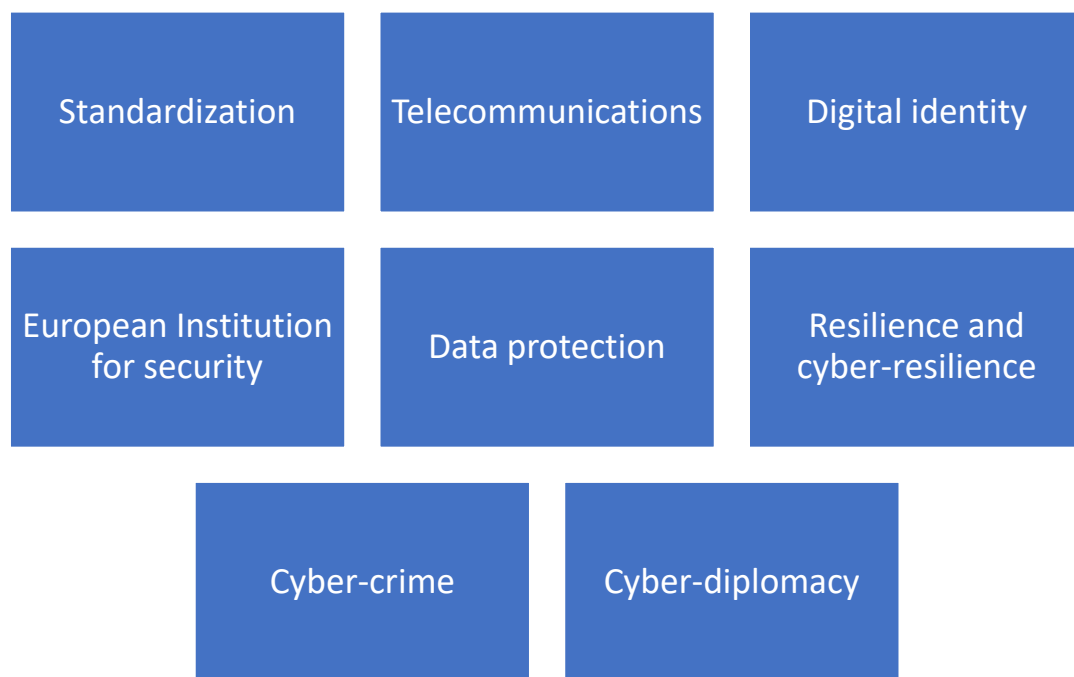


*Figure 1 - Categories of EU policies about cybersecurity*

### III EU legislation about cybersecurity

This chapter starts from the analysis and the European policies' classification in chapter I. The groups that have been identified will serve as a useful map to frame and select the binding European interventions that will be further described in the next paragraphs.

Many of these topics overlap or are consistent with the research work carried out in the Eraclito project by the Legal Research Group of the University of Genoa and of University Sant'Anna di Pisa. The exchange with technical experts has been instrumental in shaping the research approach, which is pragmatic and compliance-oriented. Special thanks are also due to the entire legal research team of the project, which provided useful opportunities for exchange and helped to consolidate the methodology behind this chapter.

Given the strong synergies with the project, it is important to clarify the scope of this chapter. While the project offers a broad perspective in line with the objective of presenting a comprehensive snapshot of cybersecurity regulation, this work is intentionally focused on the National Cybersecurity Perimeter. Accordingly, a carefully selected subset of the regulations identified in the project is examined in greater depth.

The categories adopted from chapter II are used to structure the regulations analysed in the research project, the results of which are presented in a Gantt chart<sup>273</sup>. It is the result of a cross-reading of several European sources. Firstly, all those collected in the introductory chapter. To this essential base, which mainly reflects the status quo, we have added a perspective on the future. The focus is not only on the regulations currently in force, but also on a whole series of interventions by the European legislator that are still pending. The census of proposals for regulations or directives is the result of consultation of the European Parliament's website, focusing on the periodic progress reports drawn up by the MEPs responsible for the procedures in question in the context of the "A Europe Fit for the Digital Age" strategy. In some cases, it is also possible to follow the main changes that have taken place in a given area, as the repealed regulations have been indicated and their replacements highlighted.

Although the Gantt chart was designed for different purposes, mainly related to project management, its structure is also suitable for representing the time span covered by the regulations surveyed. These are grouped into different conceptual areas, the brief description of which is given on the left, corresponding to each colour band.

At the bottom, there is a timeline showing the years at five-year intervals. Each rectangular band represents a regulation, the name of which is given in summary form, together with its numbering. The beginning and end of the band correspond to the period of validity of each piece of legislation. Normally, the end of one band corresponds to the beginning of another, so that there is always only one regulation in force. However, it sometimes happens that a piece of legislation intervenes in one or more previous pieces of legislation to amend them without replacing them. In this case, the amending interventions are represented by squares.

The use of colour also has a precise meaning. From left to right, brighter and brighter colours are used to indicate the different status of a regulation. Light grey bands represent regulations that are no longer in force, light blue bands represent regulations that are in force and darker-coloured bands represent regulations that are still in a proposed state. There are two shades of colour, red and blue. These are intended to distinguish between the hard core

---

<sup>273</sup> The graphical representation described below is included in the appendix II. This is due to the size of the image, which would otherwise have interrupted the flow of the text.



of cybersecurity regulation and those regulations that play a synergistic role in cybersecurity policy.

This choice is explained by the need to contribute to broadening the scope of cybersecurity without undermining its homogeneity. In this way, the most relevant regulations can be easily distinguished, while giving dignity to other interventions.

The distinguishing criterion used is that of "inherence". For example, it is well known that the NIS Directive<sup>274</sup> is a cybersecurity intervention, so much so that its main objective is the pursuit of a high common level of security throughout the Union. However, there are regulations that do not have the same objective, but nevertheless have a relevant impact on the compliance of the different actors. One example is the GDPR, which, in the context of the protection of personal data and the resulting fundamental rights of individuals, requires data controllers to adopt appropriate security measures. Obviously, the purpose is different, but most of the measures for the protection of personal data overlap with those for cybersecurity<sup>275</sup>. In other words, all the regulations that affect, even indirectly, security compliance are included in the scope of the census.

There are also groups of regulations related to cybersecurity that do not deal with compliance but with the preparation of the European framework, either through the preparation of common responses or through the creation of new dedicated bodies. This is the case with the so-called cyberdiplomacy toolbox or the recent creation of a cybersecurity research competence centre. All of these will be classified as related to cybersecurity, reflecting the division that will be followed throughout the chapter.

The Table 2 summarises the visual contents of the Gantt chart providing a brief description of the main legislations. Where appropriate, the main points of each piece of legislation are summarised in the fourth column from the left. Some information on the national legislation is also given. The fourth column indicates the adapting or transposing legislation. The fifth column indicates the national authority responsible for implementing and monitoring the legislation.

The aim is to equip readers with useful tools for navigating these topics, recognizing that a fully exhaustive review is beyond the scope of this work. Similarly, while the first chapter referenced a broad set of regulations, this chapter selectively addresses only the most pertinent regulations for a deeper exploration. Each regulation is addressed from the perspective most suited to highlighting its relevant aspects, ensuring that the analysis remains focused and meaningful.

The following paragraphs are not intended to serve as an exhaustive review of the area, but rather as a targeted exploration of the most relevant aspects of EU cybersecurity. Paragraph III.1 deals with a selection of current regulations that are relevant from a cyber compliance perspective. Paragraph III.2 is devoted to the NIS system, which is examined in detail, starting with the reasons that led to its creation. Its reform is introduced by highlighting the differences from the previous legislation.

### III.1 Regulations related to cybersecurity

As can be seen from the Figure 42 and Table 2, a large number of European regulations have followed in various sectors. Just as many are planned for the coming years.

---

<sup>274</sup> This topic will be dealt with in paragraph III.2.1.

<sup>275</sup> This topic will be discussed in paragraph III.1.2.1.

The selection of regulations in the following paragraphs is guided by the intention to highlight the most significant national impacts, with a particular focus on the national Perimeter. While European legislation is broad, this analysis focuses on key regulations with current and substantial relevance, excluding those where future adaptation or transposition is still pending. To effectively reconstruct established security practices within the framework of European legislation, this analysis will focus on a selection of key regulations that best reflect the Union's policies. Accordingly, telecommunications, data protection and critical infrastructure are the main topics.

The issue of telecommunications infrastructure, which has accompanied the construction of the European single market, is a perfect example of how to capture established practices. Its discussion must follow two strands: on the one hand, that of electronic communications and, on the other, that of privacy in electronic communications. This more sectoral aspect of privacy protection has always followed a separate path, which has recently continued at different speeds due to the stalling of the reform work on the so-called e-Privacy Directive. In any case, the issue of electronic communications is also central to cybersecurity, since access to network infrastructures is already a prerequisite for the existence of a security problem. The extension of the scope to OTT (over the top) operators is mentioned, which is essential to keep the regulation in line with technological progress and to bridge the gap with the second telecoms package.

The issue of privacy and data protection is a crucial next step in understanding European security practices. It reflects the sophisticated approach of the European legislator and has firmly established itself as a global standard. Considering the extensive nature of this subject, this section will concentrate on the most relevant obligations from a cybersecurity perspective to provide a clear and focused analysis. The third subject of analysis is the regulation of critical infrastructure, which has strong similarities with the NIS, with which the recent reform has continued in parallel. This is in line with the importance of critical infrastructure both in EU policy and internally.

These three regulations stand out for their broad scope, as they cover a wide range of sectors, making them particularly significant compared to other European interventions. Telecommunications involves different stakeholders, data protection is also cross-cutting, while critical infrastructure by definition involves different sectors.

Last but not least, all regulations have been subject to a more or less recent reform process. This makes it possible to review their progress and identify best practices.

Paragraph III.1.1 deals with electronic communications. Paragraph III.1.2 deals with data protection. Paragraph III.1.3 deals with critical infrastructure.

#### III.1.1 Electronic communications' framework

Electronic communications is an extremely broad field, since it encompasses all the disciplines which, through various interventions, have made it possible to liberalise and harmonise the electronic communications market. The regulation of the operation of communications networks and the creation of the basic conditions to guarantee competition between operators has been a long process, but it is essential to understand the broad outlines of the interventions in this field. Although some references have already been made in the first chapter, a more structured reconstruction is in order.

Its origin can be traced back to the European Commission's first policy analysis of the sector

in the 1987 Green Paper<sup>276</sup>. Hence, the successive regulatory acts can be divided into three 'packages'<sup>277</sup>. Starting from a situation of non-communicating markets characterised by monopoly, the first package of directives focused on creating the conditions for competition<sup>278</sup> through the entry of new players, according to the model of "service and access-based competition"<sup>279</sup>. The aim was to liberalise the various communications services, so once the common rules had been established<sup>280</sup>, a directive was issued for each of them<sup>281</sup>. Ideally, the directive<sup>282</sup> which intervened to consolidate the opening up of the market, should be seen as the end of the process. However, the following year saw the first intervention in the area of privacy in electronic communications<sup>283</sup>, after an extremely long process that had begun well into 1990 at the Commission's instigation. Even if the need for competition to be accompanied by the protection of rights had been recalled on several occasions, both by the Commission in its Green Paper<sup>284</sup> and by the Council in a number of subsequent resolutions<sup>285</sup>, it is probably no coincidence that the response came only after the

---

<sup>276</sup> European Commission, 'Towards a Dynamic European Economy, Green Paper on the Development of the Common Market for Telecommunications Services and Equipment'.

<sup>277</sup> Dalle Nogare, 'Le comunicazioni elettroniche: evoluzione del quadro istituzionale e prospettive'.

<sup>278</sup> Martin Bak, 'European Electronic Communications on the Road to Full Competition: The Concept of Significant Market Power under the New Regulatory Framework', *Journal of Network Industries* 4, no. 3 (2003): 293–324, <https://doi.org/10.1177/178359170300400303>; Jordi Gual, 'Regulation and the Development of Electronic Communications in Europe', *Info* 4, no. 3 (2002): 42–49, <https://doi.org/10.1108/14636690210440004>; Günter Knieps, 'Regulatory Reform of European Telecommunications: Past Experience and Forward-Looking Perspectives', *European Business Organization Law Review* 2, no. 3–4 (2001): 641–55, <https://doi.org/10.1017/S1566752900000653>.

<sup>279</sup> The model is based on competition between retail services because it requires the monopolist to grant access and use of its infrastructure to competitors. The concept of the dominant operator dates from this period. This is the opposite approach to the 'facilities-based competition' model, which instead relies on infrastructure competition because it encourages investment and the creation of multiple parallel autonomous networks between different operators.

<sup>280</sup> Council of the European Communities, Council Directive 90/387/EEC of 28 June 1990 on the establishment of the internal market for telecommunications services through the implementation of open network provision.

<sup>281</sup> Council of the European Communities, Commission Directive 88/301/EEC of 16 May 1988 on competition in the markets in telecommunications terminal equipment, 90; European Commission, Commission Directive 90/388/EEC of 28 June 1990 on competition in the markets for telecommunications services; European Commission; European Commission, 'Commission Directive 94/46/EC of 13 October 1994 Amending Directive 88/301/EEC and Directive 90/388/EEC in Particular with Regard to Satellite Communications', 268 OJ L § (1994), <http://data.europa.eu/eli/dir/1994/46/oj/eng>; European Commission, 'Commission Directive 95/51/EC of 18 October 1995 Amending Directive 90/388/EEC with Regard to the Abolition of the Restrictions on the Use of Cable Television Networks for the Provision of Already Liberalized Telecommunications Services', 256 OJ L § (1995), <http://data.europa.eu/eli/dir/1995/51/oj/eng>; European Commission, 'Commission Directive 96/2/EC of 16 January 1996 Amending Directive 90/388/EEC with Regard to Mobile and Personal Communications', 020 OJ L § (1996), <http://data.europa.eu/eli/dir/1996/2/oj/eng>.

<sup>282</sup> European Commission, 'Commission Directive 96/19/EC of 13 March 1996 Amending Directive 90/388/EEC with Regard to the Implementation of Full Competition in Telecommunications Markets', 074 OJ L § (1996), <http://data.europa.eu/eli/dir/1996/19/oj/eng>.

<sup>283</sup> European Parliament and Council of the European Union, Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.

<sup>284</sup> European Commission, 'Towards a Dynamic European Economy, Green Paper on the Development of the Common Market for Telecommunications Services and Equipment'.

<sup>285</sup> 'Council Resolution of 30 June 1988 on the Development of the Common Market for Telecommunications

first privacy directive<sup>286</sup>, which can be seen as a sign of continuity.

Thus, since the second package, the protection of privacy had continued in parallel with the strengthening of harmonisation. The analysis of the overall framework carried out in the context of the 1999 review<sup>287</sup> had recognised the immediate need for revision due to the development of network technologies. The first attempt at liberalisation came at a time of transition due to the spread of the Internet, when the effects of convergence were "overturning traditional market structures"<sup>288</sup>.

Internet itself was a "common platform for the delivery of a wide range of services", blurring "the distinction between voice, image and data transmission services, changing radically traditional pricing models for communications services, and challenging existing regulatory structures"<sup>289</sup>.

This also affected data protection and privacy, for which publicly available electronic communications services over the Internet presented both new opportunities and new risks<sup>290</sup>. New interventions were not long in coming, and in 2002 the second "telecoms package" was launched, which had led to a considerable simplification of the system<sup>291</sup>, with

---

Services and Equipment up to 1992' (1988), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31988Y1004%2801%29>.

<sup>286</sup> European Parliament and Council of the European Union, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

<sup>287</sup> European Commission, 'Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - Towards a New Framework for Electronic Communications Infrastructure and Associated Services - The 1999 Communications Review', 10 November 1999, COM/99/0539 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:51999DC0539>.

<sup>288</sup> European Commission, IV.

<sup>289</sup> European Commission, IV.

<sup>290</sup> See recital 5 directive 2002/58/CE: "New advanced digital technologies are currently being introduced in public communications networks in the Community, which give rise to specific requirements concerning the protection of personal data and privacy of the user. [...]".

<sup>291</sup> The reform had achieved considerable results in terms of simplification, reducing the number of legislative acts from twenty to five. See European Parliament and Council of the European Union, 'Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a Common Regulatory Framework for Electronic Communications Networks and Services (Framework Directive)', 108 OJ L § (2002), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0021>; European Parliament and Council of the European Union, 'Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on Access to, and Interconnection of, Electronic Communications Networks and Associated Facilities (Access Directive)', 108 OJ L § (2002), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0019>; European Parliament and Council of the European Union, 'Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the Authorisation of Electronic Communications Networks and Services (Authorisation Directive)', 108 OJ L § (2002), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0020>; European Parliament and Council of the European Union, 'Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services (Universal Service Directive)', 108 OJ L § (2002), <http://data.europa.eu/eli/dir/2002/22/oj/eng>; European Parliament and Council of the European Union, 'Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications)', Pub. L. No. 58, 201 OJ L (2002), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058>. For a summary of the pre-reform legislation, see European Commission, 'Communication from the Commission to the Council, the European Parliament, the Economic and

most of the previous directives being repealed. The definitions of electronic communications networks and services were considerably broadened to include telephony (both fixed and mobile), satellite, terrestrial and cable TV, as well as some related services (e.g. Application Program Interfaces or APIs). There has been a shift from the application of multiple disciplines, differentiated by means of communication, to the application of a single neutral discipline so as not to discriminate against the use of a particular technology. If convergence allowed the same service to be provided by several different means, the existence of different disciplines would inevitably lead to some media being favoured over others, thus creating distortions in the market. This is why simplification has gone hand in hand with the pursuit of a principle of technological neutrality, which in the ePrivacy Directive has been translated into a modernisation of terminology.

The changes brought about by the measures of the “third telecom package” were then added to the framework thus defined<sup>292</sup>. These had confirmed both the objectives of the legislation and the instruments used to pursue them. On the one hand, the choice was made to apply an “open access” model, which could be seen as a repackaging of the previous “open network”. On the other hand, there was the introduction of BEREC (Body of European Regulators for Electronic Communications). Despite the initial intentions, the desire to create a Community authority to ensure greater coordination and supervision met with strong resistance from governments, so that BEREC has resulted in a mere reinforcement of the ERG (European Regulators Group). After the failure of the “Connected Continent” draft regulation in 2013<sup>293</sup> due to fierce disagreements between the European Commission and the NRAs, an agreement had been reached in 2015 to adopt the “Open Internet” regulation, which at least allowed the pursuit of net neutrality and the abolition of roaming<sup>294</sup>.

---

Social Committee and the Committee of the Regions - Towards a New Framework for Electronic Communications Infrastructure and Associated Services - The 1999 Communications Review’, 18.

<sup>292</sup> The third package consists of two Directives amending the previous ones and the Regulation establishing BEREC. See European Parliament and Council of the European Union, ‘Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 Amending Directives 2002/21/EC on a Common Regulatory Framework for Electronic Communications Networks and Services, 2002/19/EC on Access to, and Interconnection of, Electronic Communications Networks and Associated Facilities, and 2002/20/EC on the Authorisation of Electronic Communications Networks and Services’, Pub. L. No. 337, OJ L (2009), <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32009L0140>; European Parliament and Council of the European Union, ‘Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 Amending Directive 2002/22/EC on Universal Service and Users’ Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on Cooperation between National Authorities Responsible for the Enforcement of Consumer Protection Laws (Text with EEA Relevance)’, Pub. L. No. 337, OJ L (2009), <http://data.europa.eu/eli/dir/2009/136/oj/eng>; ‘Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009 Establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office (Text with EEA Relevance)’, 337 OJ L § (2009), <http://data.europa.eu/eli/reg/2009/1211/oj/eng>.

<sup>293</sup> ‘Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Laying down Measures Concerning the European Single Market for Electronic Communications and to Achieve a Connected Continent, and Amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No 1211/2009 and (EU) No 531/2012’ (2013), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013PC0627>.

<sup>294</sup> ‘Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 Laying down Measures Concerning Open Internet Access and Amending Directive 2002/22/EC on Universal Service and Users’ Rights Relating to Electronic Communications Networks and Services and Regulation (EU) No 531/2012

The need for reform has recently found an outlet in the adoption of the European Electronic Communications Code in 2018<sup>295</sup>, implemented by Legislative Decree 207/2021 amending the so-called Electronic Communications Code. The new European Code modernises and recasts the directives of the second package, with the exception of the Directive on privacy and electronic communications. The regulation of the electronic communications market and the protection of privacy in electronic communications have finally gone their separate ways. While the Code is the result of effective harmonisation, the Juncker Commission had launched the procedure for a draft regulation on privacy in 2017, which has yet to be adopted<sup>296</sup>. However, at least in an ideal world, the two instruments remain implicitly linked in terms of the objectives to be pursued, which are based on the same needs arising from the technological development of electronic communications.

“Definitions need to be adjusted to ensure that they are in line with the principle of technology neutrality and to keep pace with technological development, including new forms of network management such as through software emulation or software-defined networks. Technological and market evolution has brought networks to move to internet protocol (IP) technology, and enabled end-users to choose between a range of competing voice service providers”<sup>297</sup>.

In other words, the convergence of services on Internet network protocols has favoured the proliferation of new OTT (Over The Top) operators, which, by exploiting this level of abstraction, place themselves in direct competition with traditional operators. Although this phenomenon was not unknown in the early 2000s, its scope today implies a reformulation of the definition so that regulation can adapt to this innovation, which is now the common approach<sup>298</sup>. Otherwise, there is a risk of excluding from the scope several actors that are instead clearly perceived by users as alternatives within the same market. In order to ensure effective protection for users, it is necessary to look at the functional profile of the definition of "electronic communications service", moving away from technicalities. At the same time, it should not simply be an extension, as it would be disproportionate to apply the same discipline to OTTs as to traditional operators. A new regulatory framework was needed to balance the conflicting interests<sup>299</sup>.

---

on Roaming on Public Mobile Communications Networks within the Union (Text with EEA Relevance)', 310 OJ L § (2015), <http://data.europa.eu/eli/reg/2015/2120/oj/eng>.

<sup>295</sup> European Parliament and Council of the European Union, 'Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 Establishing the European Electronic Communications Code (Recast)', 321 OJ L § (2018), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L1972>.

<sup>296</sup> The strength of the economic interests behind the new rules on the management of electronic communications metadata is a controversial issue that has been the subject of heated debate in the European Parliament and the Council of the European Union. For an update on the work, see European Parliament, 'Proposal for a Regulation on Privacy and Electronic Communications | Legislative Train Schedule', European Parliament, August 2023, <https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-e-privacy-reform>. At the moment, the legislative work is officially blocked and is no longer a priority after years of stagnation.

<sup>297</sup> See recital 14 directive (EU) 2018/1972.

<sup>298</sup> Neil Brown, 'An Assessment of the Proportionality of Regulation of "over the Top" Communications Services under Europe's Common Regulatory Framework for Electronic Communications Networks and Services', *Computer Law & Security Review* 30, no. 4 (2014): para. 2, <https://doi.org/10.1016/j.clsr.2014.05.010>; Pier Luigi Parcu and Virginia Silvestri, 'Electronic Communications Regulation in Europe: An Overview of Past and Future Problems', *Utilities Policy* 31, no. C (2014): para. 3, <https://doi.org/10.1016/j.jup.2014.03.009>.

<sup>299</sup> Brown, 'An Assessment of the Proportionality of Regulation of "over the Top" Communications Services

### III.1.1.1 Continuation regarding the security aspects

Having made the necessary preliminary remarks to define the boundaries of the electronic communications sector, it is now possible to focus on those provisions that are relevant from a cybersecurity perspective. Given the context of the study, a selection will be made, leaving out all those issues that are not specific to the subject under consideration, even if they are undoubtedly relevant at the level of internal debate<sup>300</sup>.

Although the history of electronic communications has its roots in the distant past and has gone through several phases, the issue of security has a relatively recent past, in line with the considerations made in the first chapter.

The first provisions on cybersecurity were introduced by the reform of the Third Communications Package in the so-called Framework Directive. In particular, Directive 2009/140/EC amended Article 13 of Directive 2002/21/EC by adding Article 13a. This provision focused on what, as we will see in the following paragraphs, are the key obligations for the implementation of cybersecurity, namely the implementation of risk prevention measures on the one hand and the obligation to report security incidents on the other.

In line with the scope of the Directive, the recipients of the obligations are providers of public communications networks and publicly available electronic communications services<sup>301</sup>. For simplicity's sake, the term "provider" will be used generically from this point onwards, leaving the above scope implicit.

After this essential breakdown of the article under review, the first paragraph begins with a clear reasoning based on the logic of risk management. In this sense, the introduction of technical and organisational measures must be proportionate to this prevention objective,

---

under Europe's Common Regulatory Framework for Electronic Communications Networks and Services', para. 4.

<sup>300</sup> To give just a few examples, the specific nature of the discussion means that we do not have to consider the issues of liberalising and protecting competition, of the network access models which have been developed, or even of governance and relations between operators. Let me simply draw your attention to Fabio Bassan, *Diritto delle comunicazioni elettroniche: telecomunicazioni e televisione dopo la terza riforma comunitaria del 2009* (Milano: Giuffrè, 2010); Dalle Nogare, 'Le comunicazioni elettroniche: evoluzione del quadro istituzionale e prospettive'; Giovanna De Minico, 'La risposta europea al terrorismo del tempo ordinario: il "lawmaker" e il giudice', *Osservatorio sulle fonti*, no. 2 (2017): 19; Alessandra Guerrieri, *Regolazione e concorrenza nelle comunicazioni elettroniche* (Milano, [Padova]: Wolters Kluwer : CEDAM, 2021); Federico Marini-Balestra, *Manuale di diritto europeo e nazionale delle comunicazioni elettroniche* (Padova: CEDAM, 2013); Marco Nava, *Regolamentazione e contenzioso tra operatori nelle comunicazioni elettroniche* (Torino: Giappichelli, 2012); Marco Orofino, *Profili costituzionali delle comunicazioni elettroniche nell'ordinamento multilivello*, *Collana diritto pubblico* 26 (Milano: Giuffrè, 2008); Fulvio Sarzana di S. Ippolito, *Comunicazioni elettroniche europee : Direttiva (UE) 2018/1972 5G, fibra, cybersecurity, concorrenza e tutela degli utenti*, IPSOA guida alle novità (Milano: Wolters Kluwer Italia, 2019).

<sup>301</sup> The main definitions are set out below. See Article 2 of the Directive under review, points (a) and (c):

(a) "electronic communications network means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed";

(c) "electronic communications service means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting [...]".

taking into account the state of the art, i.e. the techniques made available by the current state of technology.

The reference parameter is the impact on users<sup>302</sup> and networks, a concept that will be specified in the following paragraph, which requires the guarantee of the integrity of the network and the continuity of the services based on it. This is perfectly in line with the reference literature, since in the context of communication networks, to speak of security is to speak of integrity protection, understood in a non-specific sense as 'resilience'. In other words, the reference is not to integrity in the strict sense, but to another fundamental property of security, namely the availability of the network and the service it provides<sup>303</sup>.

In order to support the pursuit of effective integrity protection, ENISA intervened a few years after the reform of the Third Telecom Package to provide some useful guidelines to avoid a heterogeneous approach among European countries, identifying a list of twenty-five security measures taken from the reference standards and grouped into seven domains<sup>304</sup>.

In each domain, the measures are specified according to three levels of sophistication, in ascending order of protection, to provide a scale for measuring the level of compliance achieved by the standard. Although the guidelines are not always exhaustive, the logic is generally typical of the most widely used risk management standards, such as the ISO27001 family. It can therefore be said that the initial phase always involves a careful analysis of one's own assets, both in terms of technology and the human resources required, in order to define the perimeter within which the regulation must be applied.

This is followed by the implementation of the security measures deemed most appropriate, which may not be those specified by ENISA. Indeed, the last paragraph of Article 13a gives the Commission the power to adopt technical implementing measures for the purpose of better harmonisation, a possibility that has not yet been used.

Apart from the general guidance provided by Article 13b, national supervisory authorities can be considered completely free to choose the most appropriate measures. In general, they could either choose to impose the adoption of a particular standard or to consider the guidelines developed by ENISA as binding. Conversely, they could limit themselves to recommending a particular standard, without excluding other equivalent choices by individual vendors<sup>305</sup>.

---

<sup>302</sup> Note that the recipients of this protection can be both natural and legal persons, as the definition of "user" includes any "legal entity or natural person using or requesting a publicly available electronic communications service". See article 2 letter (h) of the Directive.

<sup>303</sup> P.J. Mason, 'Ensuring Network Integrity', in *IEE Colloquium on How to Compete and Connect: Understanding the Engineering of Telecommunications Network Interconnection*, 1997, 11/1-11/7, <https://doi.org/10.1049/ic:19970969>; V. Mõnton, 'Risk Assessment Methodology for Network Integrity', *BT Technology Journal* 15, no. 1 (1 January 1997): 223–34, <https://doi.org/10.1023/A:1018664103282>.

<sup>304</sup> European Union Agency For Network And Information Security, 'Technical Guideline on Security Measures', October 2014, [https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article\\_13a\\_ENISA\\_Technical\\_Guideline\\_On\\_Security\\_Measures\\_v2\\_0.pdf](https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf).

<sup>305</sup> There has always been a debate about whether to impose or recommend the adoption of standards for regulatory compliance. While adoption may seem the simplest option, as it allows the identification of clear security measures and the use of common terminology, which can also facilitate audits, it is important to remember that the target audience is very broad. In other words, since the Directive requires the application of 'appropriate' measures in a very general way, this concept must be declined for all the different providers. The result is a proliferation of existing measures to ensure proper compliance with Article 13a. This explains why it is extremely unlikely that a single standard can exhaust all the measures underlying this regulatory framework.



In any case, the existence of a common basis provided by ENISA constitutes a fundamental reference point for control activities. These activities can benefit from a clear starting point, both in terms of the level of implementation of measures and in terms of the definition of possible audit activities.

In addition to what has been examined so far, the obligation to report incidents is not secondary. Although it is now an element that has been incorporated into various regulations over time, its origins lie in the field of electronic communications<sup>306</sup>, specifically following the reform of the Third Communications Package, which intervened in both the Framework Directive and the ePrivacy Directive<sup>307</sup>.

The amendment had led to the introduction of three forms of notification. The first, and most well-known, is to the Regulatory Authority, to which each provider is required to notify incidents. An incident is defined as any breach of the integrity of the network or service, i.e. any breach of resilience, as defined above. However, not all incidents are relevant per se, as only those with a significant impact need to be reported. As the concept of significant impact is not further specified in the Directive, this issue has been left to national legislators to implement, with quite different approaches<sup>308</sup>.

This is particularly the case with regard to any specifications on the timing or content of the notification. The ENISA guidelines themselves state that they do not deal with this issue, precisely in order not to limit the freedom of the national context. However, considerable discretion has also been allowed for the other two types of notification. The second is a form of notification between national supervisory authorities where an incident has a cross-border character and may therefore be of relevance beyond national borders, perhaps because of the size of the networks or infrastructures involved or because of other factors. Finally, there is an annual form of reporting, as each authority is required to prepare a national incident report to be sent to ENISA and the European Commission. This is a monitoring system, but it is also a useful tool for gathering information on the effectiveness of the rules and the effectiveness of the measures taken by the various operators in the face of the common threat. As there is a statistical objective, despite the silence of Article 13a(3), ENISA has prepared a template for the annual report, which defines both the content and the relevance

---

This is also due to the peculiar speed with which the telecommunications sector tends to evolve, requiring the development of ever new security measures. Therefore, despite the undoubted advantages of imposing a standard, one cannot but conclude that flexibility is sometimes the most appropriate choice, especially for those Member States where providers of very different sizes coexist. For further considerations on compliance, see European Union Agency For Network And Information Security, 26–33.

<sup>306</sup> Only a few years after the reform of the Third Communications Package, similar attempts could be identified in many other European regulations, united by the need to introduce this basic security logic. ENISA intervened by carrying out a preliminary study that took stock of the various efforts and tried to understand the differences. See European Network and Information Security Agency. European Network and Information Security Agency, 'Cyber Incident Reporting in the EU - An Overview of Security Articles in EU Legislation', August 2012, <https://www.enisa.europa.eu/publications/cyber-incident-reporting-in-the-eu/@download/fullReport>.

<sup>307</sup> Although this Directive undoubtedly falls within the scope of the electronic communications sector, due to its specificity with regard to the issue of the protection of personal data, it has been placed in paragraph III.1.2.2.

<sup>308</sup> For some examples see European Union Agency for Cybersecurity, Marnix Dekker, and Karsberg, 'Technical Guideline on Incident Reporting', 7–8.

criteria for deciding which incidents should be included in the report<sup>309</sup>.

Following the recasting of the telecommunications directives with the adoption of the new European Code, the logic described above has been maintained and improved, also thanks to the experience gained in the NIS field. The new references are, respectively, Articles 40 and 41 of Directive (EU) 2018/1972, although in reality the main benefit of the new Code cannot be grasped through specific articles, as it is the result of the redefinition of the scope. More generally, as mentioned above, the complexity of the new electronic communications services, most of which take advantage of the TCP/IP protocol, has been recognised. In other words, until a few years ago, the vagueness of the definition of an electronic communications service made it extremely difficult to correctly identify the boundaries of the Regulation's application. The paradox was that very common services did not fall within the legal definition, leading to a marked fragmentation of the European market due to the different national interpretations introduced on the subject<sup>310</sup>.

BEREC had also addressed this issue by attempting to provide some sort of classification that would be useful to properly frame the issue raised by the emergence of OTT (Over The

---

<sup>309</sup> European Union Agency for Cybersecurity, Marnix Dekker, and Karsberg, 10–15. In terms of content, the report should be structured along two main lines. On the one hand, the impact of the incident, with particular attention to the services affected, the number of users involved and the duration of the incident, especially if the possibility of calling the emergency services has been obstructed. On the other hand, the cause of the incident, to be described in detail on the basis of the development of the incident itself and on the basis of the assets affected. The authority must also provide information on the response to the incident and the security measures taken after the incident. With regard to thresholds, reference is made to a relative threshold and an absolute threshold. The former takes into account the duration and number of users involved, while the latter is the product of these two values.

<sup>310</sup> The definition of an electronic communications service was found in Article 2(c) of the Framework Directive, as follows: "electronic communications service means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks". Consequently, there are three requirements that must characterise the provision of the service. Firstly, the fact that it is provided for remuneration, so that the activity is economic in nature. Indirect forms of remuneration are also included in the definition, such as revenue generated by advertising the service. Today, both case law and the European Electronic Communications Code itself are consistent in recognising the collection of personal data as a form of remuneration. See Recital 16 of the Code, which recognises that "electronic communications services are often supplied to the end-user not only for money, but increasingly and in particular for the provision of personal data or other data". The second requirement is that the service "consist wholly or mainly in the conveyance of signals on electronic communications networks". It is therefore necessary to analyse what is meant by "conveyance of signals". As a result, the notion of "transmission of signals over electronic communications networks", as defined in a number of rulings of the European Court of Justice, requires further analysis. In particular, a service can be said to be primarily based on the transmission of signals over electronic communication networks when the provider "is responsible vis-à-vis the end-users for transmission of the signal which ensures that they are supplied with the service to which they have subscribed". See *UPC DTH Sàrl contro Nemzeti Média- és Hírközlési Hatóság Elnöksége*, No. C-475/12 (European Court of Justice 30 April 2014). Although the Court's ruling has certainly widened the scope of the legislation, the greatest uncertainty has concerned the last requirement, namely whether the service is 'mainly' based on the transmission of signals over electronic communications networks. As the assessment could be made in different ways, this led to widely divergent interpretations between Member States, as there was no objective criterion to define the transmission of signals.

Top) services as opposed to traditional services<sup>311</sup>.

Although the provisions trace the previous structure introduced by the Framework Directive, it worths noting a number of updates which are in line with the changed regulatory scenario. While Article 13a did not mention any specific security measures, the new Article 40 of the Code explicitly refers to encryption as a basic tool to ensure impact minimisation. Another clarification concerns the reference to impact, which is represented not only by users and networks, but also by the services provided through them, thanks to the division made possible by the widespread use of the IP protocol. To these minor changes must be added the updated guidelines issued by ENISA, which have identified twenty-nine security measures, both technical and organisational, divided into eight domains. The Figure 2 summarises the current content.

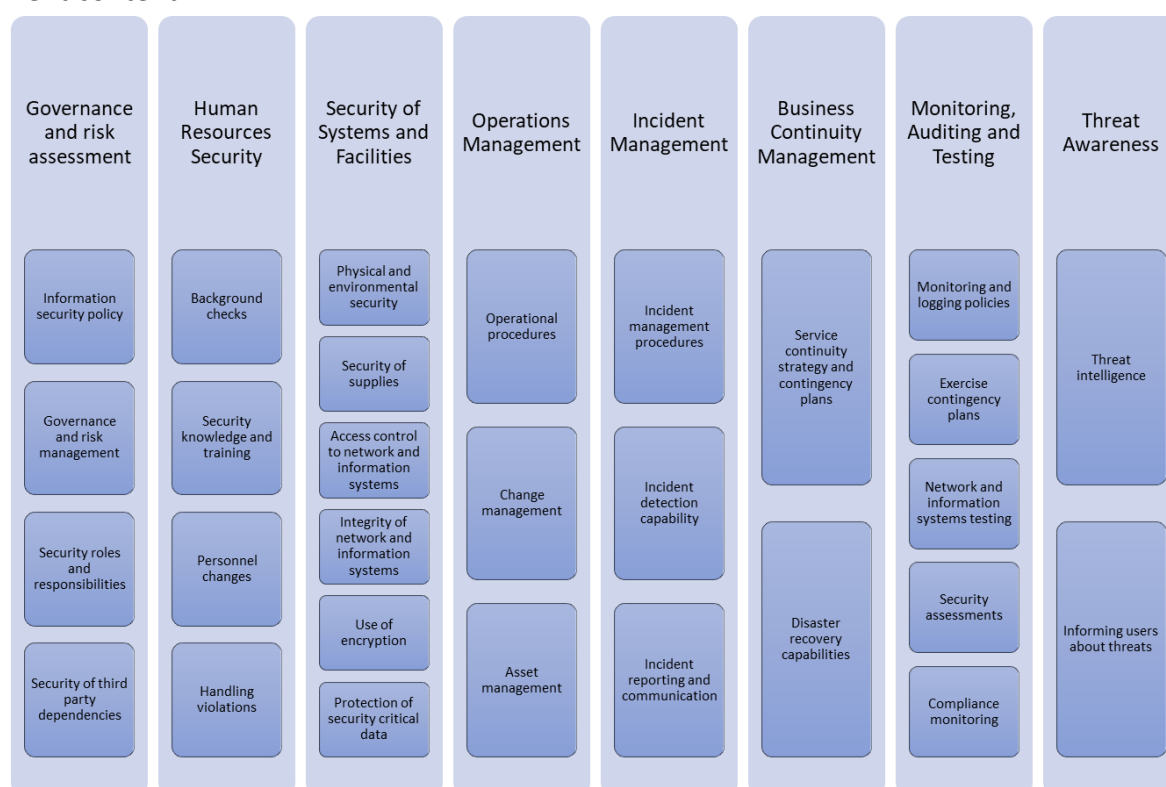


Figure 2 - Security measures domains concerning EEC

Each measure is accompanied by appropriate controls, which are useful for national authorities to verify the correct implementation of the measure. However, the overview of measures needs to be complemented by the additional controls specifically identified for operators of next generation electronic communications networks. As one of the objectives

<sup>311</sup> The BEREC report defines OTT as "content, service or application delivered to the end-user over the public Internet". This has a number of implications. Firstly, the content being transmitted does not come directly from the electronic communications provider, but from a third party using its Internet service. In addition, it is not marginal that the term OTT refers generically to a way of providing a service, without any reference to the nature of the service itself. The classification had identified three categories of OTT services. OTT-0, to be understood as those services that use the IP protocol but still fall within the definition of an electronic communications service. Hence the choice of numbering starting with 0. See Body of European Regulators of Eletronic Communications, 'BEREC Report on OTT Services', 29 January 2016, 14–17, BoR (16) 35, [https://berec.europa.eu/eng/document\\_register/subject\\_matter/berec/reports/5751-berec-report-on-ott-services](https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services).

of the new European Electronic Communications Code is precisely to support the implementation of the new 5G standard, the Directive must be read in coherence with this set of measures supporting the new 5G Action Plan. In fact, the directive itself is precisely a key step envisaged by the Commission, which was already clear in 2016 about the benefits of the transition to the new communications standard. "5G [was] seen as a game changer, enabling industrial transformations through wireless broadband services provided at gigabit speeds, the support of new types of applications connecting devices and objects (the Internet of Things), and versatility by way of software virtualisation allowing innovative business models across multiple sectors (e.g. transport, health, manufacturing, logistics, energy, media and entertainment)"<sup>312</sup>.

With this premise, the European Commission paved the way for the introduction of 5G by drawing a common map for its deployment, with adequate standardisation at European level at its heart, so as not to jeopardise its introduction. Flexibility was a key requirement, both to avoid a patchwork approach and to ensure massive deployment to support the development of the Internet of Things. Nevertheless, the Commission did not have any security concerns, at least initially<sup>313</sup>.

On the contrary, it proposed the public administration as one of the very first users, taking it for granted that "migrating public safety and security services from existing proprietary communications platforms to commercial 5G platforms [would have been] even more secure, resilient and reliable"<sup>314</sup>.

The first concerns would only become apparent with a subsequent communication, which came on the tracks of the recent European Cyber Security Strategy. Faced with a significant increase in both the quality and quantity of cyber-attacks, the Commission had defined an implementation plan that would also support the security aspects. This calls for close cooperation at both national and European level between all institutions responsible for cybersecurity under various regulations. In general terms, the aim is to assess the risks to the digital ecosystem at Union level and to take measures to mitigate them.

Three basic directions for these efforts can be identified. The first is a purely national effort aimed at measuring the telecommunications infrastructure and subsequently strengthening the security infrastructure by implementing new security obligations and measures. The results of this phase of work, which was the responsibility of each Member State, had contributed to the other two lines of work at European level.

Firstly, the national risk assessments had enabled the NIS Co-operation Group to bring together the different points of view in order to draw up a high-level security framework, highlighting common features within the Union. Although it was not a comprehensive report,

---

<sup>312</sup> European Commission, 'COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - 5G for Europe: An Action Plan', 14 September 2016, 2, COM(2016) 588 final, [https://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=17131](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=17131).

<sup>313</sup> This is despite the fact that ENISA had already prepared some initial technical security recommendations for 5G the year before. See Louis Marinos et al., 'Threat Landscape and Good Practice Guide for Software Defined Networks/5G', Threat Landscape (European Union Agency for Cybersecurity, December 2015), <https://www.enisa.europa.eu/publications/sdn-threat-landscape/@download/fullReport>.

<sup>314</sup> European Commission, 'COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - 5G for Europe: An Action Plan', 9.

it was certainly a first step towards better 5G security in the long term<sup>315</sup>.

At the same time, the results of the Member States' work also contributed to another ENISA report aimed at identifying a first threat picture for 5G networks<sup>316</sup>.

On this basis, an agreement was reached on a first set of security measures required for 5G operators, the so-called 5G Toolbox<sup>317</sup>, which represents the second line of action envisaged by the Commission, which intervened immediately after the publication of the plan to urge Member States to take rapid implementation measures<sup>318</sup>.

The Implementation Status Reports show that countries have taken concrete steps from the outset by analysing their security gaps and considering appropriate additions<sup>319</sup>. Despite the efforts of the majority, many key measures have still not been implemented by all states years later<sup>320</sup>.

With regard more directly to the regulation of electronic communications, the security guidelines published by ENISA<sup>321</sup> have also been completed for the benefit of 5G operators, following all the developments desired by the Commission.

Following the order of Article 40, some other updates can also be noted with regard to the incident reporting procedure. In general, the vocabulary used has been updated, as the vague references to “breach of security” or “loss of integrity” have been abandoned and replaced by the more specific notion of “security incident”<sup>322</sup>.

---

<sup>315</sup> NIS Cooperation Group, ‘EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks’ (NIS Cooperation Group, 9 October 2019), [https://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=62132](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132).

<sup>316</sup> The results enabled the outline of the main components of the 5G infrastructure. An initial threat assessment was detailed to identify the motives and threat capabilities of actors targeting 5G assets. The full report is available at Marco Lourenço and Louis Marinos, ‘ENISA THREAT LANDSCAPE FOR 5G NETWORKS - Threat Assessment for the Fifth Generation of Mobile Telecommunications Networks (5G)’, ENISA Threat Landscape, 5G Networks (European Union Agency for Cybersecurity, November 2019), <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks/@download/fullReport>.

<sup>317</sup> The toolbox uses the existing knowledge base to identify the main risks, on the basis of which both strategic and technical security measures are defined to mitigate them. To complement this, supporting actions are also proposed to assist the implementation of measures at national level within the framework of precise risk mitigation plans. Each Member State is invited to identify any shortcomings in the mitigation of the risks identified at national level, in order to place them among the risks defined by the toolbox. Thanks to this classification, measures can then be taken, taking into account the recommended measures. See NIS Cooperation Group, ‘Cybersecurity of 5G Networks EU Toolbox of Risk Mitigating Measures’, January 2020.

<sup>318</sup> European Commission, ‘COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Secure 5G Deployment in the EU - Implementing the EU Toolbox’, 29 January 2020, 12, COM/2020/50 final, <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2020:0050:FIN>.

<sup>319</sup> NIS Cooperation Group, ‘Report on Member States’ Progress in Implementing the EU Toolbox on 5G Cybersecurity’, 40–41.

<sup>320</sup> In particular, it highlights the risk of not applying restrictions to suppliers that are considered high risk due to their potential impact on critical assets. It is hoped that the entry into force of NIS2 and the new European Critical Infrastructure Directive will lead to a strengthening of 5G efforts. See NIS Cooperation Group, ‘Second Report on Member States’ Progress in Implementing the EU Toolbox on 5G Cybersecurity’, 22–24.

<sup>321</sup> ENISA's guidelines have been updated following the entry into force of the European Electronic Communications Code. See European Union Agency for Cybersecurity, ‘Guideline on Security Measures Under the EEC’, 7 July 2021, <https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eec/@download/fullReport>.

<sup>322</sup> See Art. 2 (42) of the European Electronic Communications Code: “Security incident means an event

Consequently, the relevance of an incident should not be understood as limited to the notion of integrity alone, but ultimately encompasses all three cybersecurity categories. Equally important is the addition of a temporal reference, albeit unspecific, requiring the provider to proceed “without undue delay”, a formula that is partly reminiscent of the approach taken by the GDPR<sup>323</sup>.

Above all, however, the clarification of the concept of “significant impact” through the introduction of a list of parameters to be taken into account is to be welcomed. Although this cannot prevent the emergence of heterogeneous interpretations at national level, it has certainly helped to maintain greater consistency<sup>324</sup>.

Finally, again in line with the GDPR, the possibility of informing affected users of threats, which was previously only ordered by supervisory authorities, is made explicit.

To summarise the main methods of notification that characterise the regulation of electronic communications, we can refer to the Figure 3.

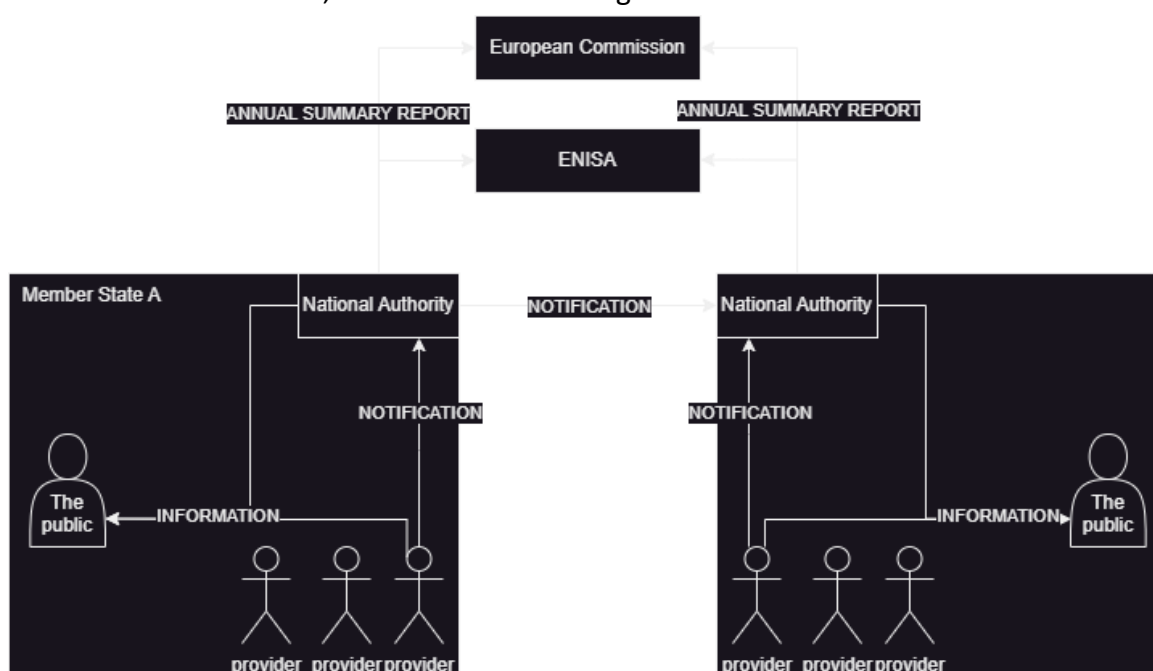


Figure 3 - Incident notification according to EEC

The last point to consider is the internal transposition of European legislation, given that the European legislator has chosen to use the instrument of a directive, albeit a recast one. With the usual delay, Italy missed the transposition deadline set for December 2020. Paradoxically, however, the delay provided an opportunity for the construction of an organic cybersecurity framework. Indeed, the following year saw the discussions that would later lead

---

having an actual adverse effect on the security of electronic communications networks or services”.

<sup>323</sup> In a certain sense, a comparison with the GDPR is possible, although the subject of the notification is clearly different. Although a time limit of 72 hours is specified, the possibility of notifying even later is left open by justifying the reasons for the delay.

<sup>324</sup> In parallel with this change, ENISA has also updated the parameters for annual reporting to ENISA and the European Commission, introducing a quantitative and a qualitative threshold. These criteria closely mirror the new legal criteria for defining impact as significant. See European Network and Information Security Agency, ‘Technical Guideline on Incident Reporting under the EEC’, 22 March 2021, <https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eec/@download/fullReport>.

to the adoption of Legislative Decree 82 on 14 June 2021, which formally sanctioned the creation of the Agency for National Cybersecurity.

Without anticipating the details here, the creation of this cybersecurity focal point had achieved considerable simplification at the country system level. In short, the new agency had immediately replaced the Ministry of Economic Development in all its cybersecurity-related functions<sup>325</sup>.

Consequently, the implementation of Article 40 of the European Telecommunications Code has also benefited from the new institutional framework<sup>326</sup>. The new wording of the article follows the Directive and assigns to ACN all the tasks previously performed by the Ministry of Economic Development. On the one hand, there is the power to determine appropriate security measures and to clarify the cases in which notification of incidents is mandatory<sup>327</sup>. On the other hand, there are inspection and sanctioning powers, which can be used to issue binding instructions. Not to be overlooked is the mention of information cooperation with other authorities at national level for incident management, in particular with the Data Protection Supervisor in the event of a personal data breach.

### III.1.2 Defining "privacy" and getting to know the underling complexity

Dealing with cybersecurity cannot be separated from an analysis of the main provisions on privacy, which, despite their undoubted differences, must be seen as complementary. This is not only a difference in aims, but more importantly a difference in basis, following the recognition of the Nice Charter as at least as valuable as the Treaties. Whereas the first Data Protection Directive shared with the NIS Directive and other cybersecurity measures the flexible basis for the creation and smooth functioning of the internal market, the new general regulation finds its foundation in Article 16 TFEU, which clearly states that "everyone has the right to the protection of personal data concerning them". This immediately highlights the different nature of the intervention, which is genetically linked to the protection of a fundamental right of the individual. The distance from rights is a characteristic shared by cybersecurity interventions, due to their technical nature.

Consider the other regulations under consideration. For example, the Critical Infrastructure Directive deals with the assessment of the security of critical infrastructure in terms of its destruction or disruption of its services, while the NIS Directive aims at a high level of security of information systems.

Undoubtedly, their objectives have a positive impact on society and individuals, since the continuity of a power plant or the information system of a hospital are clearly essential

---

<sup>325</sup> Article 16 of Law Decree 82 of 2021 clarifies that all references to the Ministry of Economic Development are to be understood as references to the Agency for National Cybersecurity.

<sup>326</sup> The transposition took place through Legislative Decree 207 of 8 November 2021, which replaced in full Articles 1 to 98 of Legislative Decree 259 of 2003, the so-called Electronic Communications Code. The purpose of the operation was to maintain consistency between the numbering of the European Directive and the new articles. It is sufficient to note that the new articles 40 and 41 follow the structure of the corresponding articles of the Directive. Previously, the provisions on security were contained in Articles 16a and 16b of the Code, which transposed Articles 13a and 13b of Directive 2002/21/EC, as introduced by Directive 2009/140/EC. At that time, the transposition had taken place by means of Legislative Decree 70 of 28 May 2012. This had also led to the establishment of the National CERT at the Ministry of Economic Development, with the task of providing technical assistance in the event of an incident report.

<sup>327</sup> As the ACN has not yet provided for this with its own provision, the provisions previously established by the Decree of the Ministry of Economic Development of 12 December 2018 remain in force. Articles 4 and 5 define the security measures and the parameters for defining an incident as significant.

services that serve the pursuit of multiple rights, but the approach is only indirect. At least on the face of it, rights are outside the scope of these rules, unlike the protection afforded to other 'immediate goods' such as the continuity of services.

Another issue that is often misunderstood is the correct declination of the term "privacy". This needs to be put in the right context to understand how it relates to the issue of cybersecurity. The term privacy is often used in the general lexicon as a generic and all-encompassing term. In fact, when we talk about privacy in a broad sense, we can understand two different and opposing rights. However, both have a common root in information about the individual.

On the one hand, privacy is a negative right. Its aim is to prevent intrusion into one's private life and thus to allow the free development of one's personality in the sphere of intimacy. The result is a constant balancing act with the right to freedom of expression.

On the other hand, the protection of personal data is a positive demand, born of the development of communication technologies, which aims to guarantee control over one's digital identity. This control can be exercised in all those new social formations, numerous and jagged, projected in the meanders of the Net. The drive that moves the two rights is opposite, inward and outward respectively, but a fundamental point of contact remains. Neither can do without the existence of effective instruments to control data.

The right to privacy in the strict sense of the word, i.e. the right to confidentiality, was first affirmed in American doctrine by Warren and Brandeis in the *Harvard Law Review*. Although many define its claim as a bourgeois pretension<sup>328</sup>, the two authors instead emphasised its human side, pointing out how the instruments for the protection of property had implemented "a recognition of man's spiritual nature, his feelings and intellect"<sup>329</sup> and how the term "property" itself had "come to encompass all forms of immaterial as well as material possessions"<sup>330</sup>.

In the Italian legal system, although doctrine and jurisprudence had for a long time provided protection, initially through the right to one's name and the right to one's image, it was not until 1975 that confidentiality was recognised as an autonomous right of personality. In any case, it is inextricably linked to freedom of expression, which poses the problem of a constant balancing act, a balance that was crystallised in the case Cass. no. 5259 of 1984.

This balance, which has found ample space in the jurisprudence, is an example of how technological evolution clearly entails the evolution of rights. An increase in the means available to freedom of expression had to be accompanied by an increase in the possibilities of privacy. In other words, over time, this negative right has acquired unprecedented declinations with respect to its origins, and has required a transformation in order to adapt to the new resilience of digital publications. It is no longer a question of the appropriateness of the publication of a piece of news, but of a dynamic adaptation of that initial balance between confidentiality and freedom of expression, which inevitably changes over time.

---

<sup>328</sup> Stefano Rodotà, 'Privacy fra individuo e collettività', *Politica del diritto*, 1974. Referring to Lewis Mumford's theories, Rodotà closely linked the private sphere to the bourgeois class, which, through a rupture in society, had claimed first property and then its own 'solitude', both as a class and as individuals. It is also interesting to compare this with medieval society, where life was collective and 'property' belonged only to the lord.

<sup>329</sup> Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy', *Harvard Law Review* 4, no. 5 (15 December 1890): 1.

<sup>330</sup> Warren and Brandeis, 1.



When public interest in a piece of news wanes, the natural yellowing that has always characterised paper publications must also be replicated in digital publications, guaranteeing the possibility of removal after a reasonable period of time.

But so far we have only discussed confidentiality, the negative side of privacy. To some extent this is related to cyber issues, where it can be declined as data confidentiality. However, the link is a distant one. In reality, cybersecurity must be guaranteed for all data, even those that do not necessarily relate to a specific or identifiable person.

The ideal dividing line between the two partially overlapping issues is the concept of personal data. The Figure 4 illustrates this overlap in the scope of a variety of regulations. On both the cybersecurity and data protection sides, we have to consider a complex system in which different sectoral regulations coexist. While the unification of cybersecurity has already been discussed in the introductory section of this chapter, it is worth making a few comments on the complexity of the data protection side. This is necessary, in particular, to avoid the misconception that the GDPR exhausts internal data protection legislation.

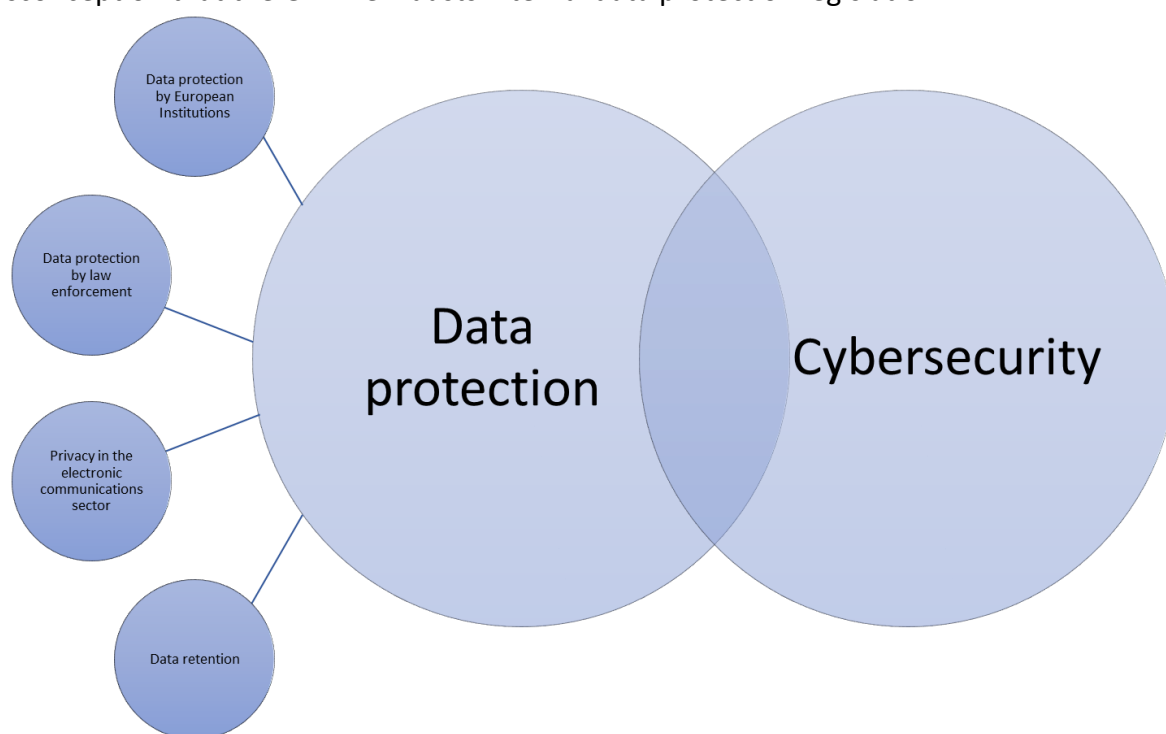


*Figure 4 Data protection regulations and cybersecurity's overlapping*

The GDPR, which replaced the previous Directive 95/46/EC<sup>331</sup>, must be placed in the area

---

<sup>331</sup> The Directive had been transposed into a series of internal laws, which were later amended and merged into the well-known Personal Data Protection Code (Legislative Decree 196/2003). Despite being replaced by a regulation, the adaptation of national legislation had not been without its delays and shortcomings. The amendment of the code for the protection of personal data, Legislative Decree 196/2003, had taken place with Legislative Decree 101 of 10 August 2018, which entered into force on 19 September 2018, months after the entry into force of the GDPR. In fact, the work had started rather slowly. Article 13 of Law No. 163 of 25 October 2017 (European Delegation Law 2016-2017) had delegated the government to intervene to expressly repeal or amend the incompatible provisions of the Privacy Code. The intervention would have been limited to what was necessary to implement the regulatory provisions that were not directly applicable. On the contrary, the breadth of the delegation allowed the executive to provide for the coordination of all the provisions in force on the protection of personal data, so that the result was a single body of law. We can therefore outline three main areas of intervention: the repeal of the incompatible provisions, the coordination of the remaining provisions

of interventions relating to internal market policies, which came under the former first pillar of the Union. This area also includes the processing of personal data by the European institutions, for which Regulation 2001/45 has recently been replaced by Regulation 2018/1725, which provides for alignment with the GDPR. There is then a plethora of European legislation dealing with the subject in relation to matters that typically fall under the other pillars. For example, under the former third pillar, there are those interventions that aim to regulate the processing of personal data in the context of police and judicial cooperation in criminal matters, first the Framework Decision 2008/977/GA, later replaced by the so-called LED (Law Enforcement Directive). This Directive (EU) 2016/680 was transposed in Italy by Legislative Decree 51 of 2018.

Finally, some exceptions to the GDPR must be taken into account, such as the area of privacy dedicated to electronic communications. Despite the long path of reform dedicated to this issue, through which the European legislator aims to achieve the amendment and replacement of the Directive on privacy and electronic communications (Directive 2002/58/EC) with a specific regulation, we are still far from an epilogue. Pending a reform, the relationship between the GDPR and e-privacy must continue to be managed on the basis of the reference in Article 95 of the GDPR, which provides for a special relationship between the directive and the regulation.

On the data retention side, on the other hand, following the annulment of Directive 2006/24/EC by the Digital Rights Ireland judgment in 2014, we are witnessing the pursuit of different approaches at European level, which in our case lead to a strong tightening of this control instrument.

Having introduced the complexity underlying the overlap between the two fields, it is now good to specify how to identify the boundary, i.e. how to distinguish when a piece of data is to be understood as personal.

Although the reference may seem outdated, many recent manuals<sup>332</sup> base the explanation of the concept of personal data on this first elaboration by the Working Party ex Art. 29, the body set up precisely on the basis of Article 29 of the first Data Protection Directive<sup>333</sup>.

---

and the bringing of the whole matter under a single corpus. The study commission at the Ministry of Justice, appointed on 14 December 2017, had only started its work on the draft decree on 4 January 2018 and completed it on 3 March 2018. The Council of Ministers approved it on 21 March 2018. The result would have led to the complete repeal of the Privacy Code, so several criticisms of unconstitutionality had been raised on the grounds of excess of delegated powers. As a result, it had become necessary to draw up a new legislative act limited to the revision of the Code. The second draft had been submitted to Parliament by the Government on 10 May. As the delegation expired on 21 May, a three-month derogation had been granted (Article 31, Law No. 234 of 24 December 2012) in order to ensure the fairness of the parliamentary debate. As a result, the special commissions had started their work on 14 May 2018 and completed it on 20 June 2018 with a positive opinion. Despite the numerous conditions, the lack of time had made it necessary to give a positive opinion, in the knowledge that further simplification measures would be necessary at a later stage. The entry into force of the GDPR on 25 May required a quick decision. In conclusion, the Data Protection Code remains today, but no longer as an implementation of the legislation, but as its completion, within the limits allowed by EU law. I refer only to Colapietro, *Il diritto alla protezione dei dati personali in un sistema delle fonti multilivello*, 95; Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali*; Franco <1946- > Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali*. 2, *Il regolamento europeo 2016/679*, I diritti nella rete della rete 4.2 (Torino: Giappichelli, 2016).

<sup>332</sup> Stefano Aterno, *Sicurezza informatica: aspetti giuridici e tecnici*, Pacini giuridica 2 (Pisa: Pacini, 2022), 22.

<sup>333</sup> Following the entry into force of the GDPR, the WP29 was replaced by the European Data Protection Board (EDPB), but its entire 20-year production was preserved by Article 94(2) of the new regulation. Quite

Its well-known opinion on the subject<sup>334</sup> can be regarded as an excellent summary of both the constant development of the case law of the European Court of Justice and the interpretative practice of the individual Member States. In particular, given the technical nature of such a sectoral issue, the opinion has the great merit of providing a very clear and modular definition, analysing each component in detail and providing various useful examples to facilitate understanding. Consequently, in view of the valuable result achieved by the Authority, it seems appropriate to recall here some of its reasoning to better clarify where to draw the dividing line between the two subjects under consideration.

The definition of personal data must be broken down into its essential elements, which must be interpreted on the basis of the objective of protecting the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with regard to the processing of personal data. The focus on fundamental rights can help to avoid an overly broad interpretation of the scope of application, where these rights are not affected by the processing. On the other hand, it can help to avoid a restrictive interpretation, linked to a mechanical application of the rules, which could lead to the persistence of dangerous grey areas.

First, it is necessary to define the concept of information, which the legislator intended to be broad, referring to "any information". Consequently, there are no exclusions based on the nature<sup>335</sup>, content<sup>336</sup> or form<sup>337</sup> of the information, which must always be taken into account.

Secondly, it is necessary to define what is meant by information "relating to a natural person". Information relates to a natural person if it is directly or indirectly related to that person. While in the first case the relationship is obvious because the information refers

---

simply, all references to the previous documentation must now be interpreted in relation to the EDPB.

<sup>334</sup> Working Party Article 29, 'Opinion 4/2007 on the Concept of Personal Data' (WP29, 20 June 2007), WP136, [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf).

<sup>335</sup> Any statement about a person, whether it is an objective statement ("Mrs. Bianchi is one metre and seventy centimetres tall") or a subjective statement ("Mrs. Bianchi is an excellent pilot"), is information. In both cases, it is not necessary to prove the truth of the statement in order to integrate the concept of personal data.

<sup>336</sup> Both sensitive data and any other type of data constitute information. Particular attention should be paid to biometric data which, on the one hand, constitute specific content of information about a particular individual and, on the other hand, constitute identifiers to link other information to a particular individual ("Mrs Bianchi has a certain genetic profile. This DNA was found in a particular place. Mrs Bianchi was probably in that place"). Although it may seem obvious by now, according to the provisions of the Charter of Fundamental Rights of the European Union and Directive 95/46/EC, information does not have to relate strictly to a person's private and family life, but may also relate to other aspects of it (e.g. working relations, economic or social behaviour). The Charter of Fundamental Rights of the European Union explicitly recognises the difference between privacy (Art. 7) and data protection (Art. 8), granting each an autonomous protection. However, in the absence of the Charter, the Directive already refers autonomously to the protection of fundamental rights, with particular reference to the protection of personal data. See article 1 (1) of directive 95/46/CE. The clarification may seem superfluous today, but when Article 8 ECHR had to be invoked in the absence of any other means of protection, the finding of an invasion of privacy was an obligatory step. In fact, even with a comprehensive reinterpretation of the concept of privacy, not all violations could automatically be prosecuted. A violation of privacy could not be protected in and of itself but had to affect the private or family life of the individual. Confirming this broad interpretation Case of S. and Marper v. The United Kingdom, No. 30562/04 e 30566/04 (European Court of Human Rights 4 December 2008).

<sup>337</sup> Information is such in any form, "alphabetical, numerical, graphic, photographic or acoustic", including digital, as made clear in recital 14 of the Directive. As far as computer data are concerned, they do not have to be contained in a database, i.e. stored in a structured way.

directly to the person<sup>338</sup>, in the second case the relationship is more complex to identify because more steps are required. For example, the information could be related to an object or a process, which in turn could be related to a person<sup>339</sup>. In any case, a relationship exists alternatively when there is a content element<sup>340</sup>, a purpose element<sup>341</sup> or an outcome element<sup>342</sup>.

Thirdly, it is necessary to clarify the concept of an 'identified or identifiable' person. A person can be said to be identified when he or she can be distinguished from the other members of a group, while he or she is identifiable when it is possible to distinguish him or her. The identification process is often complex and is carried out by means of identifiers, i.e. special information that has a close and privileged relationship with a particular person. These may be direct or indirect, depending on whether they allow identification in a direct or indirect way.

An example of a direct identifier is a person's name, which is often used in combination with other elements such as date of birth, parents' name, address and facial image. Indirect identifiers, on the other hand, are a bit more complicated, as they can never be enough to make an identification. Indirect identification is based on the combination of several identifiers. The more they are combined, the more they contribute to the uniqueness of the subject.

According to this logic, a seemingly anonymous message could still be considered as personal data, as long as it is sufficiently detailed to be traced back to the person or to other elements containing useful identifiers.

This practice is widely studied by the branch of statistics that deals with combinatorial calculus and, in particular, is fundamental for identifying the user of an electronic communication on the basis of its metadata. In this way, it is possible to isolate a particular person in order to attribute to him or her the effects of a decision that closely concerns him or her, even if one does not know his or her name or address. In fact, it is not necessary to go back to the name to define a piece of information as personal, but in the digital world the session is much more specific.

---

<sup>338</sup> A patient's clinical information relates directly and unambiguously to that patient as an individual.

<sup>339</sup> In the case of the object, information about its value could indirectly provide information about its owner in terms of wealth.

<sup>340</sup> A content element is said to be present if the content of the information relates to a particular person. For example, a patient's medical record or the data contained in their RFID badge is personal information.

<sup>341</sup> An element of purpose is said to be present when information is collected for the purpose of evaluating a particular individual, treating him or her in a particular way, or influencing his or her status or behaviour. Any collection of personal information requires a priori the definition of a purpose, which must be clearly stated in the privacy policy. This makes it possible to define certain otherwise neutral information as personal data if it is intended to influence the individual. Think of a candidate's written test, which exists to assess his or her preparation.

<sup>342</sup> An outcome element is said to be present when the information could have an impact on the person's rights and interests, although it is not intended to be used to evaluate the person or influence his or her behaviour. This situation, although similar to the previous one, should not be confused with it. The ambiguity can be clarified with an appropriate example. Consider the geolocation data of a taxi, collected for the purpose of protection against possible theft or fraud. However, the location of the vehicle also provides information about the location of its driver. Although this information is not intended to be used to evaluate the person, it may still have consequences. In other words, even if the purpose is not to evaluate the employee's performance, it is still possible to use the information for that purpose.

The process of identification is therefore a dynamic one, centred on the principle of reasonableness: "To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly"<sup>343</sup>.

In fact, the concept of identifiability cannot be defined in absolute terms, since it is a dynamic concept, from which also follows the relativity of the concepts of personal data and anonymous data. In other words, information cannot be defined as personal or anonymous in the abstract, but must always be placed in a specific situation in which the controller or processor may or may not use certain means of identification. The resulting approach is very pragmatic because it takes into account the real possibilities and therefore the real risks for the data subjects.

The reasonability then makes use of "all objective factors, such as the costs<sup>344</sup> of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments<sup>345</sup>".

In addition to these criteria, there are also those identified by the WP29 at the time, such as the benefits expected by the controller from the processing, the risks to the freedoms and rights of data subjects, or the purpose of the processing. The latter deserves clarification, as there are several situations in which data controllers process information that may not appear to be personal data. For example, a video surveillance activity for the protection of public order or the recording of a dynamic IP address to prevent the misuse of services provided over the Internet does not necessarily lead to a precise identification. Nevertheless, since the main purpose of the processing is to identify individuals, the data must be considered as personal data. This is because "it can be assumed that the controller or any other person involved have or will have the means likely reasonably to be used to identify the data subject"<sup>346</sup>.

Conversely, where the purpose of processing is not to identify subjects, appropriate technical and organisational safeguards against identification must be taken. For reasons of space, I will only touch on the breadth of pseudonymisation techniques<sup>347</sup>.

Finally, it is necessary to define what is meant by "natural person"<sup>348</sup>. However, if data

---

<sup>343</sup> See Recital 26 of Regulation 2016/679, which recalls and clarifies the previous Recital 26 of Directive 95/46/EC.

<sup>344</sup> These are the costs that must be borne in order to enable identification. If the cost would be totally disproportionate to the capabilities of the controller or processor, the data would have to be considered anonymous.

<sup>345</sup> The time parameter has to be assessed in the light of both the total duration of the processing and the state of the art. If, on the basis of the state of the art, the time needed to obtain an identification is longer than the duration of the processing, the data could be considered as anonymous. Conversely, if future technological developments can be expected to reduce the time needed for identification, this should be taken into account when deciding whether or not to classify the data as personal, even if the processing time is longer.

<sup>346</sup> Working Party Article 29, 'Opinion 4/2007 on the Concept of Personal Data', 16.

<sup>347</sup> It should be noted that pseudonymous data must also be considered as personal data, as clearly stated in recital 26 of the GDPR. See Giuseppe D'Acquisto and Maurizio Naldi, *Big data e privacy by design: anonimizzazione, pseudonimizzazione, sicurezza, i diritti nella rete della rete* 5 (Torino: G. Giappichelli, 2017).

<sup>348</sup> The reference is to every living individual, because the protection of personal data is a fundamental right of every human being as a human being. Indeed, it is human dignity that ensures that such protection is extended before and after our existence. Of course, as also stated in recital 27 of Regulation 2016/679, data protection legislation does not apply to information concerning deceased persons or persons whose existence has not yet

protection is a fundamental human right, then the term simply evokes the concept of the natural person, as reflected in Article 6 of the Universal Declaration of Human Rights<sup>349</sup>.

On the other hand, "the processing of personal data should be designed to serve mankind"<sup>350</sup>, a principle that today finds expression in the strong extension of the territorial scope of Regulation 2016/679, thus confirming the jurisprudential orientation that emerged with the Google Spain judgment.

The clarification of these criteria, which make up the concept of personal data, therefore leads to the question of whether it is possible to compare the instruments created for the protection of personal data with the more general instruments created for the protection of digital information. Given the multiplicity of regulations that can be attributed to the field of data protection, it is necessary to make a selection and focus the analysis on the most important areas. Firstly, we will analyse the system put in place following the new General Data Protection Regulation. This will be followed by a discussion of data protection in the electronic communications sector.

### *III.1.2.1 GDPR: an excerpt from the point of view of Cybersecurity*

The analysis of the GDPR can be approached from several angles. Its structure focuses, on the one hand, on the rights of data subjects, after providing some definitions and condensing some key principles that have characterised data protection since the 1980s. On the other hand, space is devoted, in a completely mirrored way, to the obligations of the controller and the processor. Given the specificity of the comparison to be made and the similarities with cybersecurity, this second part of the regulation is the most interesting for analysing the general security obligations.

These obligations can be placed within a more general principle of accountability, which has always accompanied the development of legislation since its international origins with Convention 108 of the Council of Europe<sup>351</sup>, in order to find greater specification in the new Regulation<sup>352</sup>. Although this is not a new principle, the Regulation introduces a complete reversal of the underlying logic, which can be understood through an overall analysis of the

---

come into being, but there is nothing to prevent further protection being provided by individual Member States. In short, the concept of "person" cannot be interpreted outside the national context, as well as outside sectoral rules aimed at protecting other personal rights or the rights of other persons. The same applies to legal persons, who find only minimal protection in telecommunications legislation.

<sup>349</sup> This article states that "Everyone has the right to recognition everywhere as a person before the law".

<sup>350</sup> See Recital 4 Reg. 2016/679 and its precedent in Recital 2 Dir. 95/46/EC. See Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González., No. C-131/12 (European Court of Justice 13 May 2014). This judgment broadened the concept of establishment, as the processing of personal data was considered to be part of establishment activities, since the controller had opened a branch in a Member State in order to provide services to individuals in its territory.

<sup>351</sup> Council of Europe, 'Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data', 28 January 1981, <https://rm.coe.int/1680078b37>. The Convention has been recently updated. For further information see 'Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data' (Consiglio d'Europa, 18 May 2018), [https://search.coe.int/cm/Pages/result\\_details.aspx?ObjectId=09000016807c65bf](https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf); 'Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data' (Consiglio d'Europa, 10 October 2018), <https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a>; 'The Modernised Convention 108: Novelties in a Nutshell' (Consiglio d'Europa, 2018), <https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8>.

<sup>352</sup> Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali*, 275–84.

obligations to protect personal data. Compared to the initial lack of explicit provisions on the subject, this has resulted in a system that devotes an entire chapter to the obligations of the controller and the processor.

Whereas the Directive only required the controller to comply with data quality principles in general, the Regulation went further and required compliance to be substantiated by adequate documentation<sup>353</sup>.

This can now be defined as a first feature of the principle of accountability. A second aspect emerges from the addition of other accountability statements, such as the guarantee of an adequate level of security of personal data against unauthorised processing, which, since the Regulation, has risen to the level of a fundamental principle of data protection<sup>354</sup>.

Previously, the owner was also obliged to take appropriate safety measures to prevent certain risks, but this was only a specific obligation. Its renewed importance corresponds to an important change in logic.

Whereas the previous system was based on *ex ante* control, with notification and prior checking by the supervisory authority<sup>355</sup>, the Regulation introduces an *ex post* system, which means constant monitoring by the national authorities, greater powers and, above all, greater responsibility on the part of the controllers. There has been a shift from a system of deresponsibility, based on prior control by the authority, to a system in which control rests with the individual controller, who must design the processing in such a way as to concretise the principles of personal data protection. In this way, data protection has moved "from theory to practice", just as the WP29 called for when it expressed its views on the accountability principle<sup>356</sup>.

The GDPR has undoubtedly adopted the proposals made on that occasion, introducing a general principle that does not specify the measures to be taken, but rather the criteria for determining them in the specific case. Article 24 is, in fact, a general formula applicable to all data controllers and to all processing operations, since it simply requires the adoption of appropriate technical and organisational measures to ensure and demonstrate compliance with the regulation<sup>357</sup>.

Article 32 on security measures should therefore not be misunderstood, as the security measures listed are general and only examples. The controller can and must take all the measures he deems appropriate to mitigate the level of risk inherent in the processing. Both

---

<sup>353</sup> Compare Article 6(2) of the Directive with Article 5(2) of the Regulation.

<sup>354</sup> See article 5(1)(f).

<sup>355</sup> See Articles 17, 18 and 19 of Directive 95/46/EC, as transposed in Title VI Part I of our Data Protection Code. The controller had to notify the Garante of the processing operations listed in Article 37 in the manner set out in Article 38. In addition, the prior authorisation of the Garante was required for the processing of sensitive data, unless the processing was already covered by specific general authorisations.

<sup>356</sup> Working Party Article 29, 'Opinion 3/2010 on the Principle of Accountability', 13 July 2010, WP173, [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf).

<sup>357</sup> See article 24(1): "Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary". It should be remarked how the article perfectly recalls recital 74: "Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons".

provisions leave a wide margin of manoeuvre, which makes it possible to reaffirm the principle of technological neutrality in the protection of personal data<sup>358</sup>.

Whereas before the controller was limited to applying the minimum safeguards set out in the Code in a one-size-fits-all manner, today the controller is not only free to choose data protection techniques but must also design the process so that it itself complies with the Regulation<sup>359</sup>.

Nowadays we often talk about privacy by design, i.e. data protection at the design stage of processing. Technology cannot be taken as it is, but must be designed and adapted to the principles of personal data protection. The change is particularly clear when looking at Annex B of the previous Personal Data Protection Code, which specified the minimum security measures to be taken. From this perspective, the controller was allowed to adapt the processing to the available technology.

With privacy by design, on the other hand, we have moved from processing by technology to technology for privacy, from technology as a constraint to technology as the key to privacy. It also reflects the principle of minimisation, because in the absence of personalisation by the user, only the data that is strictly necessary for the purpose should be collected<sup>360</sup>. In short, it can be stated that the entire system of the GDPR is based on accountability.

Based on this key reading, some further considerations can be made. First, the introduction of appropriate security measures for risk prevention is discussed, which can be seen as a common feature of cybersecurity regulation. On closer inspection, however, the risks considered in the two areas are measured against two rather different yardsticks. For example, while the risk identified by the NIS Directive relates to the operation and continuity of essential and digital services, the risk identified by the GDPR instead relates to the destruction, loss, alteration, unauthorised disclosure of or access to personal data stored or otherwise processed<sup>361</sup>.

---

<sup>358</sup> This principle can be also found in recital 15: "In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. [...]".

<sup>359</sup> See the articles of Part I, Title V of the Personal Data Protection Code. Chapter II sets out a series of minimum measures that must be adopted for each processing operation, depending on whether it is carried out with the aid of electronic instruments, Art. 34, or without, Art. 35. Chapter I, on the other hand, spoke in general terms of security measures "to minimise ... the risks ... typical of the processing" [original Italian text: "in modo da ridurre al minimo ... I rischi ..."]. Although this provision was very similar to the current Art. 32 Reg. 2016/679, it did not lead to effective accountability due to the mild sanctions. The minimum measures were effective, not only because they were standard and inexpensive to apply, but above all because their absence was punishable by up to two years' imprisonment under Art. 169. Adequate measures, on the other hand, corresponded to an administrative fine of between ten and one hundred and twenty thousand euros, ex Art. 162, which could simply be written off as a cost of doing business. Instead, the Regulation refers to "implement appropriate technical and organisational measures, [...] which are designed to implement data-protection principles, [...] in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects". On closer inspection, this is a repetition, because the implementation of the Regulation makes it possible both to give concrete expression to the principles of data protection and to protect the rights of the persons concerned. In short, it would have been sufficient to refer to compliance with the Regulation, as Article 24 does, since these are overlapping perspectives. See article 25(1) GDPR.

<sup>360</sup> See article 25(2) GDPR.

<sup>361</sup> The WP29 identified three different typologies of privacy risk, one for each cybersecurity property "confidentiality breach" Working Party Article 29, 'Opinion 03/2014 on Personal Data Breach Notification'



In other words, in the first case, the risk is parameterised to an object, i.e. the ability of a service to autonomously overcome possible incidents. Only in the second case, on the other hand, is there any consideration of the individual, or rather of the consequences that may have an impact on his or her freedoms. This is a normal consequence of the different objectives pursued by the two regulations, the measures of which can then be placed at two different points in time. In this sense, measures for the cybersecurity of an organisation are prior to those for the protection of personal data, which certainly do not end with the adoption of the former. To be even clearer, the same security measure could contribute to compliance with both the NIS and the GDPR, but data protection compliance can never be exhausted by cybersecurity measures<sup>362</sup>.

A number of additional and specific obligations in the area of IT security illustrate the greater breadth of obligations under the GDPR.

These include the Data Protection Impact Assessment (DPIA) tool, which, after its origins in environmental law, found its way into privacy law in the early 2000s with the support of the doctrine<sup>363</sup>. The instrument must be understood as all-inclusive, i.e. capable of adapting to the specificities of each processing operation in order to describe its status, risk level and, therefore, possible countermeasures. Although widely used, it was initially only a voluntary tool and only with the GDPR has it become mandatory. This is consistent with the risk-based approach mentioned above<sup>364</sup>, which is used by the European legislator to introduce a threshold above which the DPIA is considered mandatory. The rationale is in line with the principle of empowerment of the data controller, who must therefore be free to make the choices he deems most useful to best prepare the processing. Accordingly, Article 35 of the GDPR only requires a mandatory DPIA when the processing is "likely to result in a high risk to the rights and freedoms of natural persons".

As pointed out by the WP29, this implies an initial prudence on the part of the data controller, in particular to consider the introduction and potential impact of new technologies. It should be noted that the Article does not provide clear and objective criteria

---

(WP29, 25 March 2014), 5, WP213.

<sup>362</sup> Alfonso Contaldo and Davide Mula, *Cybersecurity law: disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche* (Pisa: Pacini giuridica, 2020), 154–58.

<sup>363</sup> Roger Clarke, 'Privacy Impact Assessment: Its Origins and Development', *Computer Law & Security Review* 25, no. 2 (January 2009): 123–35, <https://doi.org/10.1016/j.clsr.2009.02.002>; Adam Warren et al., 'Privacy Impact Assessments: International Experience as a Basis for UK Guidance', *Computer Law & Security Review* 24, no. 3 (January 2008): 233–42, <https://doi.org/10.1016/j.clsr.2008.03.003>; David Wright, 'Should Privacy Impact Assessments Be Mandatory?', *Communications of the ACM* 54, no. 8 (August 2011): 121–31, <https://doi.org/10.1145/1978542.1978568>; David H. Flaherty, 'Privacy Impact Assessments: An Essential Tool for Data Protection', in *New Technologies, Security and Freedom* (Annual Meeting of Privacy and Data Protection Officials, Venice, 2000), <https://aspe.hhs.gov/privacy-impact-assessment-essential-tool-data-protection>.

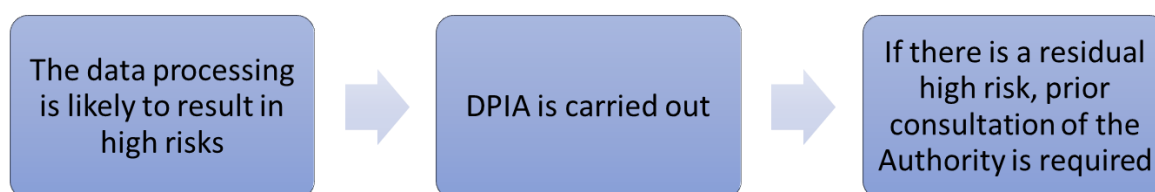
<sup>364</sup> As this is not the place for an analysis, reference is made to the extensive doctrine on the subject. See R. Gellert, 'We Have Always Managed Risks in Data Protection Law', *European Data Protection Law Review* 2, no. 4 (2016): 481–92, <https://doi.org/10.21552/EDPL/2016/4/7>; Raphaël Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation', *Computer Law & Security Review* 34, no. 2 (April 2018): 279–88, <https://doi.org/10.1016/j.clsr.2017.12.003>; Milda Macenaite, 'The "Riskification" of European Data Protection Law through a Two-Fold Shift', *European Journal of Risk Regulation* 8, no. 3 (September 2017): 506–40, <https://doi.org/10.1017/err.2017.40>; C. Quelle, 'The "Risk Revolution" in EU Data Protection Law: We Can't Have Our Cake and Eat It, Too', *Cybersecurity*, 11 July 2017, <https://www.semanticscholar.org/paper/The-%E2%80%98Risk-Revolution%E2%80%99-in-EU-Data-Protection-Law%3A-We-Quelle/4bd00e31cb2965ba67c5471e4f02573e2db4c5dd>.

to determine with certainty where the DPIA should be carried out, but only provides an atypical set of examples<sup>365</sup>.

This explains the proposal of the WP29 to carry out the impact assessment of the processing in any case, if there is any doubt about the "high impact" of the processing. On the other hand, it is always a useful tool for the controller, who must always ensure the security of the processing, and can therefore use it both for individual processing operations and for several operations if they are similar. Ideally, it should be carried out prior to the start of the processing, as it is a preparatory exercise to highlight any criticalities in the processing. Consequently, the DPIA should be conceived as a dynamic moment to be repeated over time, rather than as a one-off exercise. Despite its importance, the GDPR does not provide a precise definition of this process, but only some minimum contents<sup>366</sup>.

The reason for this may be found in the desire not to crystallise a single approach, but to give each holder the flexibility needed for his or her own treatment, adding any other "modules" that may be useful for the final documentation<sup>367</sup>.

The only certainty in the variability of possible methodologies is their two-stage structure. A first one describing the processing with its purposes and its risks for the rights of the data subjects, and a second one identifying appropriate security mitigation measures. It is precisely the result of such mitigation that allows a correct interpretation of the meaning of the following article on prior consultation of the authority. Although this possibility is never excluded, it becomes mandatory when, even after the identification of appropriate mitigation measures, the processing operation would still present a high risk of affecting fundamental rights.



---

<sup>365</sup> Article 35 (3) define three examples: a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing; b) processing on a large scale of special categories of data; c) a systematic monitoring of a publicly accessible area on a large scale. These cases are further enriched by some criteria developed by the WP29. To recall the most relevant ones: the process of social scoring of a data subject; systematic monitoring; the processing of data of a highly personal nature; the processing of data concerning a vulnerable data subject. It should be emphasised that the WP29 adopted a very broad approach, going beyond the traditional concept of sensitive data and referring to "data of a highly personal nature". These are data that must be considered as sensitive as the others, even if they are not included in the legal definition. Think about financial data or employment status data.

<sup>366</sup> See article 35(7).

<sup>367</sup> Felix Bieker et al., 'A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation', in *Privacy Technologies and Policy*, ed. Stefan Schiffner et al., vol. 9857, Lecture Notes in Computer Science (Cham: Springer International Publishing, 2016), 21–37, [https://doi.org/10.1007/978-3-319-44760-5\\_2](https://doi.org/10.1007/978-3-319-44760-5_2); Katerina Demetzou, 'Data Protection Impact Assessment: A Tool for Accountability and the Unclarified Concept of "High Risk" in the General Data Protection Regulation', *Computer Law & Security Review* 35, no. 6 (November 2019): 105342, <https://doi.org/10.1016/j.clsr.2019.105342>; Michael Friedewald et al., 'Data Protection Impact Assessments in Practice: Experiences from Case Studies', in *Computer Security. ESORICS 2021 International Workshops*, ed. Sokratis Katsikas et al., vol. 13106, Lecture Notes in Computer Science (Cham: Springer International Publishing, 2022), 424–43, [https://doi.org/10.1007/978-3-030-95484-0\\_25](https://doi.org/10.1007/978-3-030-95484-0_25).

If up to now we have been talking about a system aimed at preventing risks, we must also consider the GDPR's ability to react when such a risk materialises. Apart from the novelties introduced in terms of sanctions, one of the most relevant institutions for the comparison we want to develop is certainly that of data breach, which was previously implemented only in the sectoral sphere.

Not only did the previous Directive not provide for this, it even lacked a definition of the concept of a data breach. In line with the empowering approach of the GDPR, the obligation to notify incidents is universally recognised as a necessary step to assess the preparedness of each data controller. In other words, if each is responsible for planning processing by preparing the most appropriate security measures from the outset, there must be consistent accountability when these tools prove insufficient to prevent the onset of risk. However, this is not just a 'punitive' obligation, because, as the WP29 also emphasises, the data breach mechanism should not be seen in isolation, but as an integral part of the incident response plan. It creates an important moment of exchange with the supervisory authority, which can intervene to provide useful advice to the holder on how best to handle the incident. At the same time, notifications provide an important flow of information that can be used to improve response strategies and develop effective processing security policies.

Article 33 describes this as an obligation on the part of the data controller, which must be carried out without undue delay and, where possible, no later than seventy-two hours after the data controller becomes aware of the incident. This means that the GDPR does not set an upper time limit within which notification must be made. As the rest of the provision makes clear, the seventy-two hours should not be seen as an insurmountable limit, but as a recommended time, provided that the delay is accompanied by the reasons for the delay. Again, in line with the desire to hold controllers accountable, they will be required to adequately justify their decision to delay compliance by demonstrating that the delay does not affect the personal data, but rather aims to better prepare the notification. For example, a data controller may have started an investigation following the discovery of a personal data breach and discover several other similar breaches. Investigating each of these breaches could result in a longer investigation period for the purposes of a "mass" notification of all such breaches<sup>368</sup>.

Of course, there is nothing to prevent such a notification from being made within seventy-two hours if possible, thus relieving the burden of justifying the delay, but one can understand that this type of notification is characterised by long delays. However, in the face of these situations, the justification of the delay is not the only tool provided by the GDPR. According to the reasoned interpretation offered by the WP29, it opens up the practice of multi-stage notification, typical of those breaches where it is impossible to have all the necessary information before a thorough investigation. Accordingly, the holder may make a notification by providing the minimum information at its disposal and informing the authority in advance that future updates will be made in the form of a follow-up, in parallel with the further

---

<sup>368</sup> Working Party Article 29, 'Guidelines on Personal Data Breach Notification under Regulation 2016/679' (WP29, Ottobre 2017), 16, WP250rev.01. Even if a recent version of the guidelines has been published by EDPB (European Data Protection Board) in 2023, I prefer to refer to the original version, since the text has almost been left untouched. For the updated version, see European Data Protection Board, 'Guidelines 9/2022 on Personal Data Breach Notification under GDPR', 28 March 2023, [https://edpb.europa.eu/system/files/2023-04/edpb\\_guidelines\\_202209\\_personal\\_data\\_breach\\_notification\\_v2.0\\_en.pdf](https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf).

investigation of the affected systems. This is also a way to avoid unduly delaying the initial contact and to benefit from any suggestions on how to handle the incident. On the other hand, the downside of this practice is that there is an overabundance of initial information. Of course, there is no sanction for reporting an incident that does not subsequently turn out to be a personal data breach. However, from the perspective of the authority, overzealousness may overshadow more relevant notifications. These two reporting methods are summarised in Figure 6.

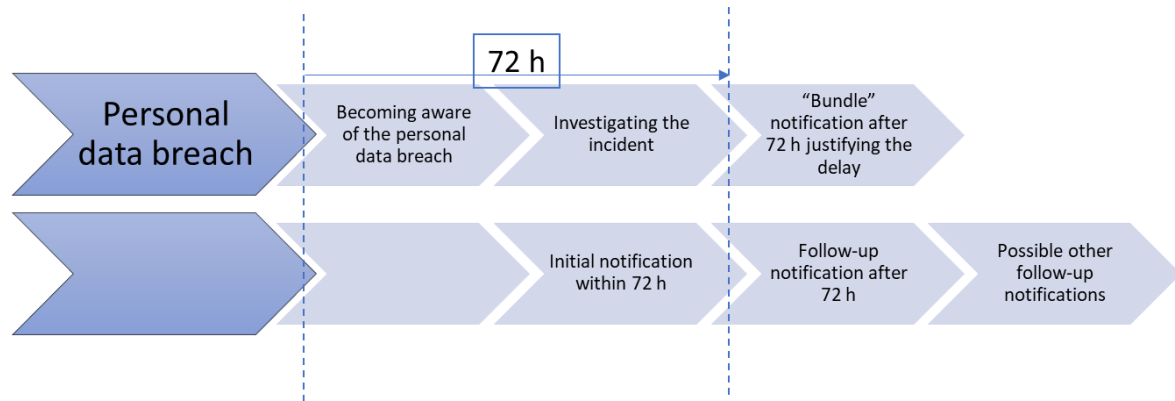


Figure 6 - Data breach notification procedure in the light of GDPR

In both cases, it is crucial to understand what is meant by a personal data breach, which can be explained as any violation of the fundamental properties of information security<sup>369</sup>.

As a result, the cases for notification appear to be quite broad, since, at least on the surface, even the breach of a single asset is sufficient. In fact, the GDPR introduces a threshold below which the notification procedure is not required, contrary to previous interpretations of the WP29, which instead tended to provide the authorities with as complete an overview of each incident as possible. Indeed, the wording of the provision makes it clear that notification must be made "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons"<sup>370</sup>.

The result is a pragmatic approach to the problem, with the aim of further empowering the data controller. Not only does the controller need to have appropriate measures in place to prevent breaches, but he or she also needs to be able to assess whether the breach is relevant. This is in line with other relevant institutions, such as the DPIA described above, which require the controller to have a clear idea of both the likelihood of the risk occurring and the severity of the risk associated with a processing operation before it is carried out<sup>371</sup>.

<sup>369</sup> Referring to the definition introduced by the GDPR: "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". See art. 4 (12). The three attributes of information security are commonly represented by the acronym CIA, which stands for Confidentiality, Integrity and Availability. Analysing the definition, destruction of data would result in a loss of availability, alteration would result in a breach of integrity and unauthorised access would result in a breach of confidentiality. This is in line with the WP29's earlier reading, which had reconstructed an initial definition of data breach using these three attributes. See footnote 361.

<sup>370</sup> Working Party Article 29, 'Guidelines on Personal Data Breach Notification under Regulation 2016/679', 10.

<sup>371</sup> See recital 75 and 76 of GDPR. This general indication of the GDPR is enriched by some criteria identified by the WP29 to assess where there is a risk to the fundamental rights of data subjects. For example, the following are identified: a) the nature of the breach, since the breach of the confidentiality of health data is certainly more serious than the loss of its availability; b) the sensitivity, nature and volume of the data involved; c) the ease

For example, a breach involving the confidentiality of personal information that is already in the public domain is unlikely to cause harm. Similarly, the loss of a device containing data that has been properly encrypted in accordance with appropriate security standards is unlikely to cause harm, provided that the encryption key has not been compromised and cannot reasonably be obtained.

In addition to the need for a risk management capability, it is important to be able to identify the point at which the owner can reasonably be expected to be aware of the breach. This expectation is in line with the requirement of Article 24 of the GDPR, which states that appropriate security measures must be taken in a manner that demonstrates compliance with the regulation. Their selection must therefore also take into account the need for notification, which implies the ability to detect an ongoing breach in a timely manner<sup>372</sup>.

Certainly, however, the controller can be said to be aware of a breach when it notifies the authority, thereby fulfilling its obligation under Article 32(2) GDPR. In this way, the role of the data controller emerges, who must inform the data processor without undue delay, so that the latter can notify the authority within the next 72 hours, after having carried out the appropriate risk assessments. Although no specific timeframe is indicated for this internal information, there is nothing to prevent the controller from regulating this case more strictly by introducing specific contractual obligations on the controller.

To conclude this series of considerations on data breaches, it is worth mentioning a second hypothesis, that of a breach notification to the data subjects, in addition to the notification to the supervisory authority. Article 34 of the GDPR introduces this institution, which is the consequence of a higher risk threshold.

While the data controller must notify the supervisory authority whenever there is a risk to the fundamental rights and freedoms of individuals, notification to data subjects requires a high risk. The rationale is not to place an additional burden on the controller when the conditions do not necessarily require the cooperation of the data subjects to mitigate the risk posed by the breach. In addition, no precise time limit is imposed, only that it must be done without undue delay, provided that the data subject can be located.

The European legislator also takes into account the particular burden of contacting the data subject by proposing alternative means where compliance would be disproportionate. Reference is made to the possibility of public communication, which can inform individuals in an equally effective way, by choosing instruments that maximise the likelihood of reaching the data subjects concerned. In any case, the choice of the most appropriate means must be made in close contact with the supervisory authority<sup>373</sup>, which may also require the controller to proceed with the disclosure even if it does not identify a high risk. Special needs must also be taken into account where the specific breach gives rise to a presumption that a criminal offence has been committed. In such situations, the legitimate interest of the judicial police authorities not to be unnecessarily hindered in their investigative activities must be

---

with which individuals can be identified from the data involved; d) the severity of the consequences for individuals; e) the particular characteristics of the data subjects or the data controller concerned, who may be vulnerable individuals or data subjects with a high degree of sensitivity; f) the number of individuals involved.

<sup>372</sup> For example, logging and detection systems could be implemented at the endpoints as well as on the networks where processing takes place, in order to maximise awareness of one's own systems.

<sup>373</sup> See recital 86 GDPR.

respected<sup>374</sup>.

There are other exceptions that can be explained in the light of the desire to link any performance by the controller to a risk-based reasoning. Similarly to what has been said about notification to the supervisory authority, the adoption of a priori or a posteriori security measures capable of avoiding the materialisation of the high risk would render useless the notification<sup>375</sup>, which must be conceived as a tool to enable the data subject to adopt the necessary behaviour to protect himself<sup>376</sup>. In any event, if the holder chooses not to disclose, adequate documentation must be maintained to support the reasons so that the lack of necessity can be assessed.

### *III.1.2.2 Privacy in the field of electronic communications*

Article 4 of Directive 2002/58/EC introduced an obligation for providers of electronic communications services to take technical and organisational measures appropriate to the risk, possibly in conjunction with the network provider. This provision was introduced in parallel with Article 17 of Directive 95/46/EC, not only because of the similarity of the wording, but also because the latter was its interpretative parameter<sup>377</sup>.

At least initially, the obligations were rather general. They were limited, on the one hand, to taking reasonable steps to mitigate the risk and, on the other hand, to informing subscribers of the particular risks that existed and the countermeasures to be taken to mitigate them, where these went beyond the normal safeguards that the provider was required to take.

Obviously, the provision had to be placed in the binary structure of our Privacy Code, which divided between minimum security measures and reasonable security measures. In other words, the measures specifically foreseen for providers of electronic communication services had to be added to the minimum measures foreseen for any processing by electronic means.

Today, following the adaptation of the Code to the GDPR, it is necessary to refer to Article 32 of the GDPR, which, as already mentioned, gives the data controller complete freedom to decide on the adoption of adequate measures, thus overcoming the dichotomy between the two levels of protection.

In addition, the repeal of the whole of Title V of the Privacy Code made it necessary to move the provisions relating to providers of electronic communications services by means of a specific revision of Article 132 of the Code<sup>378</sup>. Despite having relocated, all the rules simply continue to apply.

Having said that, it is possible to describe the main obligations in this area. In particular,

---

<sup>374</sup> See recital 88 GDPR.

<sup>375</sup> Again, an example of a priori security might be the use of encryption, while an example of remediation might be changing the credentials of compromised users before they are used by attackers.

<sup>376</sup> In fact, the minimum content of the notice is to indicate the measures recommended to minimise the likely consequences of the breach.

<sup>377</sup> See recital 20 of the directive 2002/58/EC: "Security is appraised in the light of Article 17 of Directive 95/46/EC".

<sup>378</sup> The provisions on the security obligations of providers of electronic communications services were first implemented in Article 32 of the Code, which was later amended following Directive 2009/136/EC, which also introduced Article 32-bis. Now, following Legislative Decree 101/2018, the provisions of Article 32 have been merged into Articles 132-ter ("Security of processing") and 132-quater ("Risk information"). The absence of a specific article replacing Article 32-bis is explained by the entry into force of Regulation 611/2013.

after repeated reminders from the WP29<sup>379</sup>, the European legislator intervened with a substantial amendment to introduce the indication of minimum measures<sup>380</sup>.

As a result, in addition to the reference to the measures of the Data Protection Directive, which continue to apply, the obligation to limit access to only those personnel necessary for authorised purposes and certain typical risks has been added. These were useful in defining the concept of adequate protection<sup>381</sup> and are largely reminiscent of the logic inherent in the GDPR. No less important was the introduction of a data security policy, a useful moment of compliance at a time when data protection rules were perceived only as a bureaucratic obstacle.

However, the most important innovation was the obligation to notify the data breach authority, an obligation first introduced with the third reform package and then standardised by Regulation 611/2013, which has similarities to the general obligation currently in force through the GDPR, which was discussed in the previous section. The Figure 7 summarizes the main steps of the notification procedure to the DPA.

---

<sup>379</sup> Working Party Article 29, 'Opinion 2/2008 on the Review of the Directive 2002/58/EC on Privacy and Electronic Communications (ePrivacy Directive)' (WP29, 15 May 2008), WP150, [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp150\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp150_en.pdf); Working Party Article 29, 'Opinion 1/2009 on the Proposals Amending Directive 2002/58/EC on Privacy and Electronic Communications (e-Privacy Directive)' (WP29, 10 February 2009), 4–6, WP159, [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp159\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp159_en.pdf); Working Party Article 29, 'Opinion 7/2000 On the European Commission Proposal for a Directive of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector of 12 July 2000 COM (2000) 385', 2 November 2000, 5, WP36, [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp36\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp36_en.pdf).

<sup>380</sup> The reference is to the intervention of the Third Telecoms Package, in particular Directive 2009/136/EC. This intervened to amend Directives 2002/22/EC and 2002/58/EC. It is worth highlighting the amendment of Article 4 of the ePrivacy Directive to introduce paragraphs (b) and (c). The former refers to the implementation of certain minimum security measures, which are listed exhaustively, such as restricting access to authorised personnel, protecting stored or transmitted data against access, destruction or alteration, and implementing a security policy. The second additional paragraph refers to the notification of data breaches. See Alessandro Mantellero, 'Si rafforza la tutela dei dati personali: "data breach notification" e limiti alla profilazione mediante i "cookies"', *Diritto dell'informazione e dell'informatica*, 2012; Marie-Andrée Weiss, 'Towards Mandatory Data Breach Notification Laws in the European Union', *Journal of Internet Law* 14, no. 12 (2011): 24–29.

<sup>381</sup> See article 4 (1bis) of directive 2002/58/EC, as amended by directive 2009/136/EC: "protect person al data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure...".

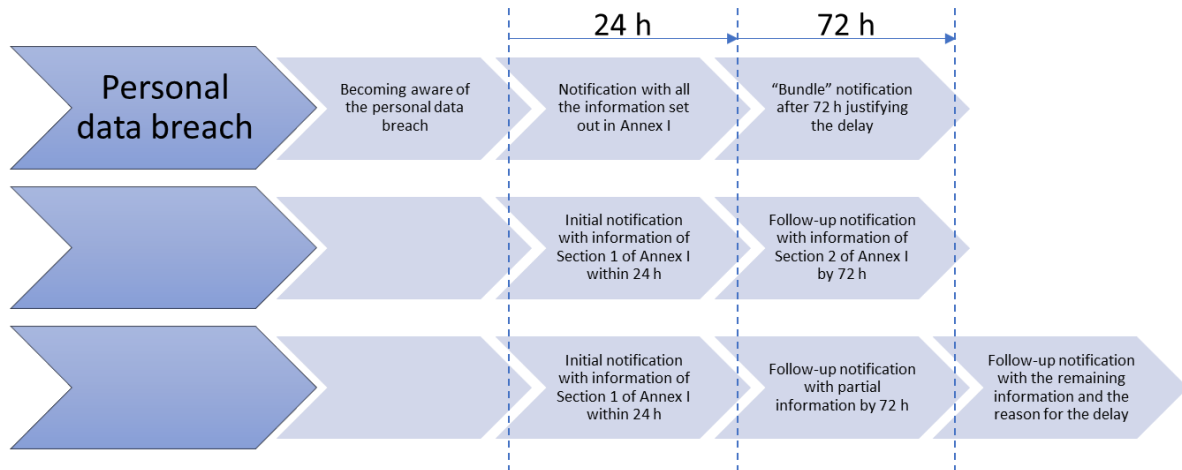


Figure 7 - Data breach notification according to regulation 611/2013

The fact that there are marked similarities is evidence of the institution's origin in the electronic communications sector. Any provider of electronic communications services is obliged to notify the DPA (Data Protection Authority) immediately of any data breach. In addition, if the breach is likely to affect the personal data or privacy of a subscriber or other person, they must also notify them.

Apart from a few formalities<sup>382</sup>, there is perfect consistency with the GDPR, which also separates the notification to the guarantor and the communication to the data subjects. The only notable observation is the greater rigidity of the e-privacy discipline, according to which notification is always mandatory. As already examined, the GDPR introduces exceptions to notification where the impact on the rights and freedoms of natural persons is unlikely.

While the absence of exemptions apparently allows for a better quality of supervision, there are also implicit risks. Firstly, there is a significant lack of responsibility on the part of providers of electronic communications services and networks, as the notification of each event implies a lack of adequate risk assessment and knowledge. From this point of view, it goes against the principle of responsibility, which is instead exalted by the GDPR, which would like to see an ideal effort towards risk assessment in the preparation of processing. Secondly, there is a dangerous overburdening of the data protection authority. It is true that, in the abstract, a comprehensive view of incidents might allow a better understanding of the threat scenario, but such an analysis requires the presence of a large number of dedicated staff and, above all, the appropriate expertise. The same reasoning applies to the communication procedure to the data subject, or more precisely to the user or subscriber.

Although both the GDPR and e-privacy refer to data subjects, it is important to note that different terminology is used. While the GDPR simply uses the term “data subjects”, e-privacy

<sup>382</sup> For example, the GDPR's timeframe is 72 hours from the date of discovery of the breach, while the e-privacy discipline is only 24 hours, with a further 72-hour extension if further investigation is required. Both disciplines allow for a two stage notification to the Garante, which in the latter case is mandatory, in the event of an extension of time. The first notification must be made within 24 hours and the second within 72 hours. More details can be found in Figure 6. In terms of content, the e-privacy notification is more detailed in order to adapt to the needs of the subject matter. The mandatory contents are listed in Annexes I and II of Regulation 611/2013. In addition, it was commendable to provide a secure electronic tool for service providers to ensure both the security of the notification and that it is carried out in a structured format. See Recital 19 of Regulation 611/2013, which refers to the XML format.



refers to “the subscriber or other person”. Initially, the data subject was only the subscriber, but following criticism from the WP29<sup>383</sup>, the current wording was adopted to extend protection to all individuals who see their data held by the service provider, even if they are not subscribers at the time of the breach.

Although both regulations allow for an exception to disclosure if technical safeguards have been taken in advance to render the data unintelligible, there remains a difference in the degree to which disclosure is mandatory. The GDPR requires disclosure only when there is a “high risk to the rights and freedoms of natural persons”, whereas ePrivacy simply requires it “when the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual”<sup>384</sup>. Despite the common existence of an exception, which partly helps to reduce the bureaucratic burden on operators, the stringency of the obligation must be measured against the conditions for its application.

The exasperation of this approach had been supported by the WP29<sup>385</sup>, which had even opposed the creation of an exception in order to favour the highest degree of awareness of the data subjects, contrary to the European Data Protection Supervisor<sup>386</sup>.

It needs to be remembered that in the digital society, breaching is a common and absolutely physiological phenomenon. A lack of exceptions, especially if the criteria are too broad, would risk exposing individuals to constant communication and creating unnecessary anxiety. This could lead to an unjustified mistrust of certain services, perhaps simply characterised by excessive zeal.

### III.1.3 Critical infrastructures

#### III.1.3.1 *Origins and the European debate*

The issue of critical infrastructure was closely intertwined with the European policy efforts analysed above. Although only a few references have been made to this issue in the context of the various policies that have followed, it is worth recalling the main steps that led to the current regulations.

The first aspect to consider is the disconnect between the issue of infrastructure and that of its protection. Vulnerable infrastructures have existed for a long time, but it is only in the recent past that they have started to be considered as “critical infrastructures”. In this sense, critical infrastructures are not a new innovation, because change is not to be sought in the individual physical element itself.

The problem can only be grasped by looking at the whole. “The increasing interest in CI reflects the changing conditions of post-modern societies in terms of technological development, growing interdependences and related threat perceptions. [...] There tends to be a correlation between the developmental level of society, the number and complexity of critical infrastructures and the severity of the society’s vulnerability to a loss of supply”. There is a directly proportional relationship between the increase in the complexity of society and

---

<sup>383</sup> Working Party Article 29, ‘Opinion 2/2008 on the Review of the Directive 2002/58/EC on Privacy and Electronic Communications (ePrivacy Directive)’, 3.

<sup>384</sup> See article 34 (1) of the regulation (EU) 2016/679, article 4 (3) of the amended directive 2002/58/EC, as specified by articles 3 and 4 of the regulation 611/2013.

<sup>385</sup> Working Party Article 29, ‘Opinion 1/2009 on the Proposals Amending Directive 2002/58/EC on Privacy and Electronic Communications (e-Privacy Directive)’, 7.

<sup>386</sup> European Data Protection Supervisor, ‘Second opinion on ePrivacy’, gennaio 2009, 31–38, [https://edps.europa.eu/sites/edp/files/publication/09-01-09\\_epricacy\\_2\\_it.pdf](https://edps.europa.eu/sites/edp/files/publication/09-01-09_epricacy_2_it.pdf).

the increase in the latent vulnerabilities inherent in the interconnections between different sectors and assets.

This is what made it possible to increase the number of victims after the terrorist attacks long before 11 September. The new tendency of terrorism to target critical infrastructures can explain the new attention that had characterised the topic on both sides of the Atlantic. In fact, “by attacking these means of mass transit, communication and power distribution, it is possible to cripple western cities (albeit on a relatively temporary basis) and, in certain cases, also ensure a high loss of life in the attack”<sup>387</sup>.

Despite the phenomenon of privatisation, which had removed much of the infrastructure from public control, joint public-private action was needed more than ever to tackle the problem<sup>388</sup>. This was necessary not so much for the infrastructure itself, but to take account of another aspect brought about by the change brought about by the advent of the new wave of terrorism in the old continent.

Contrary to what has just been pointed out about the increasing complexity of society, this change goes to a deeper level, that of the political, social and cultural significance attributed to the infrastructure. “The cultural and political significance of infrastructure is precisely what makes it critical, what makes it a critical infrastructure. [Therefore, it is correct to assume that] all critical infrastructure has cultural and political significance”<sup>389</sup>. “It is not the reality of a computer virus in itself, but rather the fear of the release, the presence of a negative symbolic virus, the contagion of insecurity, which disseminates distrust and fear, both in the world of private commercial services around which the European society is organised, but also in terms of international trust and faith in a globalised market system”<sup>390</sup>.

Despite the fact that terrorism had, at least initially, increased the commitment to protect the European project, “the European has been a far less evocative and far less idealistic or spiritual concern for European commonality: the fate of Europe’s shared critical infrastructure”<sup>391</sup>.

Having briefly outlined the reasons why the concept of critical infrastructure is relatively new, notwithstanding the older origins of major European and national infrastructures, its earliest origins can be traced back to the United States in the mid-1990s. Indeed, the evolution of the concept overseas may help to understand the evolution of the definition. Confirming what has just been theorised, at an early stage the main concern was the deterioration of the infrastructure, so much so that only the term ‘infrastructure’ was used. It was only when people began to think in terms of vulnerability to more or less unforeseen events that the debate took on the importance it has today. In general, “the criteria for an infrastructure to be judged critical became that it must be vital to one or several broad national functions”<sup>392</sup>.

---

<sup>387</sup> Arjen Boin and Denis Smith, ‘Terrorism and Critical Infrastructures: Implications for Public-Private Crisis Management’, *Public Money and Management* 26, no. 5 (November 2006): 296, <https://doi.org/10.1111/j.1467-9302.2006.00543.x>.

<sup>388</sup> Boin and Smith, 296.

<sup>389</sup> J. Peter Burgess, ‘Social Values and Material Threat: The European Programme for Critical Infrastructure Protection’, *International Journal of Critical Infrastructures* 3, no. 3–4 (January 2007): 479, <https://doi.org/10.1504/IJCIS.2007.014121>.

<sup>390</sup> Burgess, 481.

<sup>391</sup> Burgess, 471.

<sup>392</sup> Christer Pursiainen, ‘The Challenges for European Critical Infrastructure Protection’, *Journal of European*

Even if the concept of CI has different meanings in different times and places, “there seems to be a trend towards a broad, holistic understanding of CI, where it is understood as networks or systems of vital functions of the society as a whole or the infrastructures embedded in these functions”. The fruits of that debate would be imported to the Old Continent through the medium of NATO influence after 11 September<sup>393</sup>.

This would lead to a proliferation of interventions by the European institutions, building on the system established by the 1997 Treaty of Amsterdam, which had helped to create the conditions for strengthening the Union's fight against terrorism. The Tampere European Council in 1999 and the Santa Maria de Feira European Council the following year were devoted to this issue and defined measures to promote integration in the field of security and justice.

"The four intervening years since the attacks in New York and Washington witnessed a flurry of political activity, beginning with the adoption in the European Council of a "Proposal for a Council Framework Decision on Combating Terrorism" and leading through a rapid evolution to the release, on 17th November 2005, of a Green Paper on a EPCIP"<sup>394</sup>.

While the proposal sanctioned terrorism as "a threat to democracy, to the free exercise of human rights and to economic and social development"<sup>395</sup>, there were a number of other actions in between, some of which have already been mentioned.

First, the statement by the Council of the European Union, which recalled the common nature of the terrorist threat. "A terrorist act against one country concerns the international community as a whole. [...]. No country in the world can consider itself immune. Terrorism will only be defeated by solidarity and collective action"<sup>396</sup>. In particular, some commentators have pointed out that "by underscoring the notion of 'solidarity' in Article 2 of the "Declaration on Combating Terrorism" the European Council also sets out the primary precondition for advancing the concept of European critical infrastructure, namely the interconnectedness of European commerce and livelihoods through transnational infrastructures"<sup>397</sup>.

Several other targeted interventions by the European Commission followed in the same year, e.g. the communication and the communication<sup>398</sup>.

One of these was specifically related to critical infrastructure, highlighting how terrorism exploits the widespread cascading failures made possible by the synergistic effects of an industry's infrastructure on one another. "Critical infrastructures consist of those physical and

---

*Integration* 31, no. 6 (1 November 2009): 723, <https://doi.org/10.1080/07036330903199846>.

<sup>393</sup> Pursiainen, 723.

<sup>394</sup> Burgess, 'Social Values and Material Threat', 472.

<sup>395</sup> European Commission, 'Proposal for a Council Framework Decision on Combating Terrorism' (2001), 1, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52001PC0521&qid=1691393731226>.

<sup>396</sup> Council of the European Union, 'Declaration on Combating Terrorism', 25 March 2004, 1, [https://www.consilium.europa.eu/uedocs/cms\\_data/docs/pressdata/en/ec/79637.pdf](https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/79637.pdf).

<sup>397</sup> Burgess, 'Social Values and Material Threat', 474.

<sup>398</sup> European Commission, 'Communication from the Commission to the Council and the European Parliament - Preparedness and Consequence Management in the Fight against Terrorism', 20 October 2004, COM(2004) 701 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52004DC0701&qid=1687082120625>; European Commission, 'Communication from the Commission to the Council and the European Parliament - Prevention, Preparedness and Response to Terrorist Attacks'.

information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States”<sup>399</sup>.

Although some general criteria such as the scope, the magnitude or the effects of time of a potential incident have been theorised for the identification of critical infrastructure, this concept can only be negative. “What is in essence critical about critical infrastructure is based on what may be the result of the critical infrastructure being lost or damaged”<sup>400</sup>.

However, the most significant progress has been driven by the conclusions of the Council of the European Union, which invited the Commission to prepare a comprehensive strategy to improve the protection of critical infrastructure<sup>401</sup>.

That request led to the Green Paper on a European Programme for Critical Infrastructure Protection to collect useful feedback for the forthcoming institution of the European Programme for Critical Infrastructure Protection (EPCIP), whose goal is “to ensure that there are adequate and equal levels of protective security on critical infrastructure, minimal single points of failure and rapid, tested recovery arrangements throughout the Union”<sup>402</sup>.

This was not only an essential step in the development of awareness of the problem, but also an opportunity to demonstrate the breadth of the European concept of infrastructure, which should not be limited “to the material objects or facilities from whose loss we might suffer”<sup>403</sup>. In this respect, it is possible to see how semiotic protection, which can also consider intrinsic value, has been promoted<sup>404</sup>.

Despite the progress of the debate at European level and the subsequent response to the terrorist phenomenon, which led to the proposal of the first European Directive on the identification of critical infrastructures, many shortcomings remained.

While the increasing interconnectedness of the systems made it possible for more incidents to occur, the tensions in society and the political climate had increased the pressure on political leaders. The decline in tolerance of failure, accompanied by the dangerous debate about Western over-tolerance of minorities, had led to the adoption of symbolic measures to satisfy public opinion rather than effective mechanisms<sup>405</sup>. The paradox was that people wanted reliable, cost-effective and secure systems, but an efficient system was not necessarily more secure and reliable. Everyone wanted to prioritise security, but no one

---

<sup>399</sup> European Commission, ‘Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the Fight against Terrorism’, 3.

<sup>400</sup> Burgess, ‘Social Values and Material Threat’, 475.

<sup>401</sup> Council of the European Union, ‘Presidency Conclusions – Brussels, 17 and 18 June 2004’, 17 June 2004, 4, <https://data.consilium.europa.eu/doc/document/ST-10679-2004-REV-2/en/pdf>.

<sup>402</sup> European Commission, ‘Green Paper on a European Programme for Critical Infrastructure Protection’, 3.

<sup>403</sup> Burgess, ‘Social Values and Material Threat’, 478.

<sup>404</sup> Burgess, 481.

<sup>405</sup> Boin and Smith, ‘Terrorism and Critical Infrastructures’, 297–98. Citing the word of the authors: “A terrorist attack presents policy-makers with dilemmas that have impossible choice dimensions: everybody looks at them to ‘do something’, but it is far from clear what that ‘something’ is or whether it is even possible to achieve without causing additional harm. Managers are required to manage ‘ahead of the curve’ in a way that both anticipates the potential for harm associated with their (in)actions, as well as ensures that the decisions taken do not create greater problems further down the timeline”.

wanted to spend more<sup>406</sup>.

A brief look at the situation in Italy reveals similar problems, accompanied by widespread backwardness in this area. To recall just a few significant episodes, the European Programme for the Protection of Critical Infrastructures, launched in 2005, was preceded by a series of seminars convened by the Commission with the aim of promoting the exchange of best practices and gathering useful information. To this end, a questionnaire had also been circulated among the Member States, with the request to reply within the following year. Unfortunately, apart from the fact that Italy did not participate in the events at that time, it was not even able to reply to the questionnaire, which was based on the assumption that all states had already set up a coordinating body at national level. Together with Greece and Malta, Italy shared a tragic state of inability to perceive its own security posture, caused by ignorance of its own infrastructure and strategic importance<sup>407</sup>. All previous national initiatives to address the problem of IT infrastructure had little impact or were ignored<sup>408</sup>. There was a clear lack of capacity to coordinate between the different actors at national level.

### *III.1.3.2 The first directive on critical infrastructures*

After several non-binding interventions, which served the Commission to gather feedback, the work led to the first proposal for a directive in 2006. “There exist a number of critical infrastructures in the European Union, which if disrupted or destroyed, would affect two or more Member States. It may also happen that failure of a critical infrastructure in one Member State causes effects in another Member State. Such critical infrastructures with a trans-national dimension should be identified and designated as European Critical Infrastructures (ECI). Because of the trans-national dimension [...] an integrated EU-wide approach would usefully complement and add value to the national programmes”<sup>409</sup>. The European Union's intervention was urgently needed to ensure the uniform and consistent implementation of measures in this area. “[That was] becoming increasingly likely as new technologies and market liberalisation [meant] that much infrastructure [was] part of a larger network. In such a situation protection measures are only as strong as their weakest link”<sup>410</sup>.

The proposal is also interesting for its ability to reconstruct existing regulatory interventions in this area. The interconnectedness of infrastructures made it difficult to intervene without considering the regulatory basis. Although it would go beyond the scope of this paper to go into the details of the different sectors, suffice it to say that several interventions in the IT sector were considered in synergy with the Critical Infrastructure

---

<sup>406</sup> Boin and Smith, 301.

<sup>407</sup> Carlo Sarzana Di Sant'Ippolito, ‘I Problemi Delle Infrastrutture Critiche Informatizzate’, *Diritto Dell'Internet*, no. 4 (2007): 2.

<sup>408</sup> Examples include the report commissioned by the then Minister for Innovation and Technology and published by the inter-ministerial working group in 2004, or the study promoted by ISCOM (Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione) in the same year. Meanwhile, a special office called CERT-GOV has been set up at the CNIPA (National Centre for Information Technology in Public Administration) to monitor and prevent computer incidents in the public sector and to provide operational support in the event of alarms or ongoing situations relating to computer incidents. However, the government of the day failed to confer any real institutional status on the organisation, so that its real activity was limited to the dissemination of alerts.

<sup>409</sup> European Commission, ‘Proposal for a DIRECTIVE OF THE Council on the Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve Their Protection {SEC(2006) 1648} {SEC(2006) 1654}’ (2006), 2, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52006PC0787>.

<sup>410</sup> European Commission, 3.

Directive<sup>411</sup>.

Although the definition of critical infrastructure was not so different from those already circulated with the first communications, and not so different from the definition in the final text of the first directive, it was certainly in a different regulatory context.

First of all, the proposal had a rather broad scope, which was put forward with the ambition of creating strong coordination on a European basis in a crucial area. Therefore, the definition, although not particularly different in itself, would have been much more far-reaching due to the larger number of sectors initially included in the scope.

Second, and no less important, was the more specific approach to the risk, which, at least at the outset, had been conceived in terms of the terrorist threat alone.

While the final text of the Directive would have drastically reduced its scope, it would have generalised the approach to risk, rather than limiting it to the consequences of terrorist attacks<sup>412</sup>.

When reading the text of the Directive, some clear indications can already be found in the recitals. A first clarification, also reiterated by the Council, concerns the European competence to intervene in this matter. While the responsibility for organising measures to protect infrastructures lies always and exclusively with the Member States, the Union can and must intervene to establish clear procedures for identifying infrastructures of European importance, as laid down in Article 5 of the Treaty on European Union and article 352 TFEU.

This is indeed the purpose of the legislation, as is the development of a common approach to improving infrastructure protection.

The first point to note is that the definitions clearly distinguish between the concepts of Critical Infrastructure and European Critical Infrastructure. Critical infrastructure is any infrastructure that is essential for the maintenance of essential government functions and the disruption or destruction of which would have a significant impact on a Member State. The two concepts share the same risk rationale, but the distinguishing criterion is the extent of the impact, which in the latter case must affect at least two Member States. It is infrastructure of European importance that is at the heart of the legislation.

For their identification, the Directive outlines a fairly precise procedure, defined in a number of passages in Annex III, which can be regarded as a kind of explanation of Article 3. Each step represents the successive application of selection criteria, which in turn reduces the choice from the initial set. Firstly, all infrastructures falling within the two sectors covered by the Regulations, energy and transport, as defined in Annex I, must be identified. Then, all the resulting infrastructures have to be verified on the basis of the two definitions. In other words, it has to be verified whether they are critical or not and whether criticality can be identified

---

<sup>411</sup> The proposal mentioned interventions in the following areas: IT sector, health sector, financial sector, transport sector, chemical sector, and the nuclear sector. In the IT sector, the telecommunications package is mentioned, together with the Council Decision on attacks against information systems and the Regulation establishing ENISA.

<sup>412</sup> On the other side of the Atlantic, however, the United States favoured the opposite principle. This was true both at the beginning, when the focus was on deliberate threats, and especially after the events of 11 September, which would further strengthen this approach with the creation of the National Strategy for Homeland Security. It was only after the disasters caused by Hurricane Katrina in 2005 that a more general approach to risk would emerge. The strategy formulated in 2006 would indeed have adopted a generalised approach to risk. See Pursiainen, 'The Challenges for European Critical Infrastructure Protection', 730–31.

across borders. Finally, some cross-border criteria must be applied<sup>413</sup>.

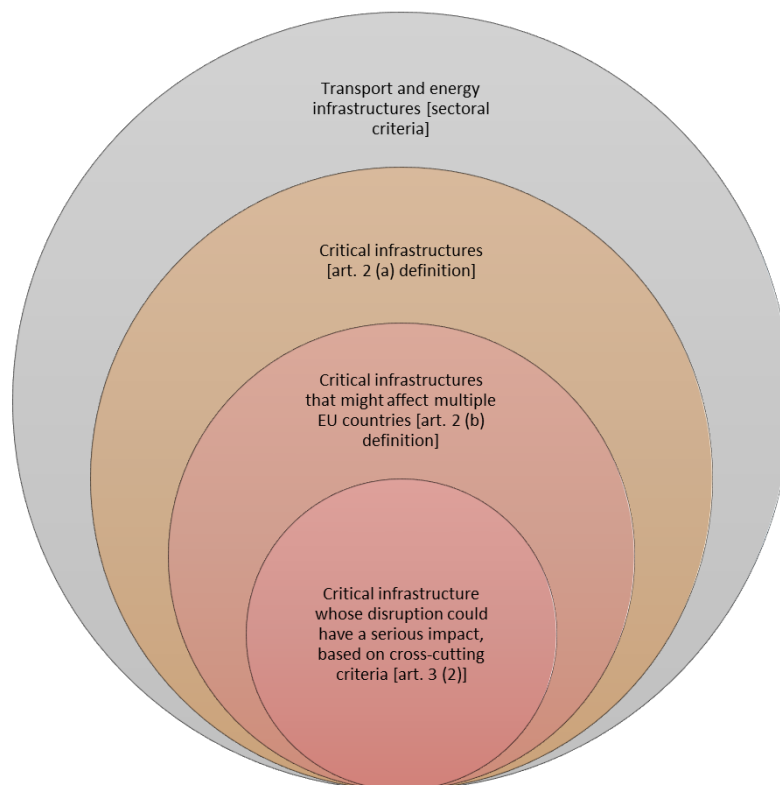


*Figure 8 - Scope of the first Critical Infrastructures Directive (Council Directive 2008/114/EC)*

As shown in the picture, only a small circle of infrastructures can be identified as European Critical Infrastructures.

Critical infrastructure is identified through bilateral or multilateral discussions between Member States. When each of them identifies an infrastructure as critical, they must contact those Member States that could be significantly affected based on the assessment made. European Critical Infrastructures are designated on the basis of the results of the agreement. Operators of such infrastructure are promptly notified of the designation so that they can fulfil their legal obligations. Their main obligations are to draw up a operator security plan (OSP) and appoint a security liaison officer. Each operator shall promptly identify all its assets and, consequently, the security measures in place for their provision, in accordance with the minimum content prescribed in Annex II.

Although this obligation is vaguely reminiscent of those recently introduced in Italy for perimeter subjects, the rules were much more flexible, not requiring the adoption of typical security measures, but simply the performance of a periodic risk analysis. Moreover, this obligation should be fulfilled in the case of equivalent national sectoral rules, leaving the door open for significant national differences.

The other aspect is the appointment of a security liaison officer to act as a contact point between the operator of the identified infrastructure and the national control authority of the Member State.

Each Member State must set up an authority to act as a contact point for coordination at

---

<sup>413</sup> The following non-exhaustive criteria result from Article 3 in conjunction with Annex 2: the severity of impact, the availability of alternatives, the duration of the recovery, the casualties criterion, the economic effects criterion, and the public effects criterion.

national level, with other Member States and with the Commission, and to ensure regular reporting of the results of the annual risk analyses carried out in each sub-sector.

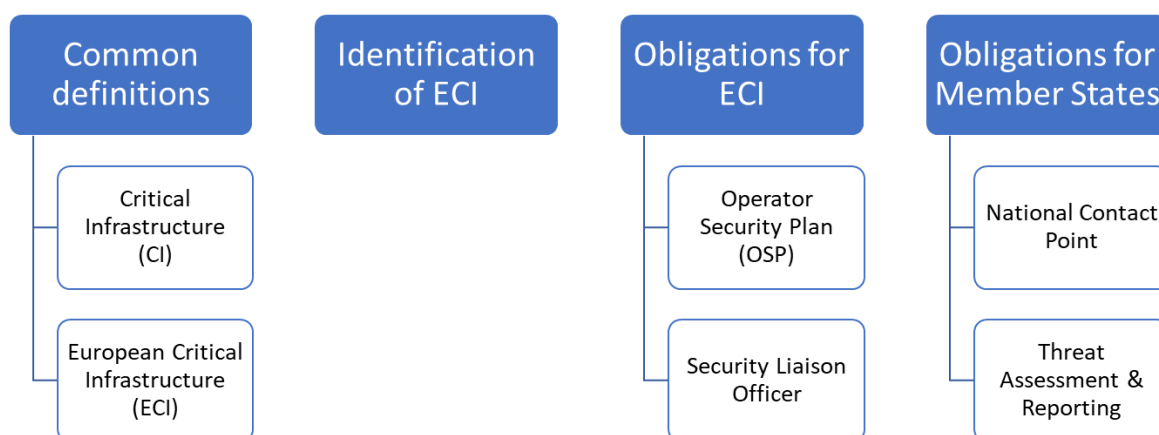


Figure 9 - Summary of the first Critical Infrastructures directive

Italy would also transpose the Directive, but this was not the only attempt to contain the problems of critical infrastructure. Italy, following the Western experience, had readily equipped itself with provisions, mainly of European matrix, to contain and contain the main problems, but without creating a specific centralised and coordinated discipline<sup>414</sup>.

Broadly speaking, the national regulation follows the European one, so it is useful to focus on the main differences introduced by the Italian legislator.

The first lies in the peculiar choice of introducing a definition of infrastructure alongside that of critical infrastructure. While this may have its own logic, the definition proves to be too vague, to the point of being superfluous<sup>415</sup>.

Another addition is the concept of sectoral infrastructure, which should be understood as a homogeneous field of activity, by theme, in which infrastructures operate, which can be further subdivided into subsectors. Note that the term "sectoral" refers to the field of activity, which must be homogeneous, and not to sectors or sub-sectors. In fact, the definition of "intersectoral" does not contradict that of "sectoral", but partially overlaps with it, since it includes any activity that affects two or more sectors or subsectors. Despite the fact that Italy is very backward in this field, this distinction shows an awareness of the interdependence of several critical infrastructure sectors or subsectors.

Equally noteworthy is the distinction between external negative effects, such as loss of operation, and intrinsic effects, which involve damage to infrastructure or the surrounding environment. This implied a focus on environmental heritage that was missing from the Directive.

The final point concerns the designation of the competent national authority, which, according to Article 4, is the Ministerial Situation and Planning Team (NISP), which acts as the

<sup>414</sup> Alfonso Contaldo and Flaviano Peluso, 'La Protezione Delle Infrastrutture Critiche Nell'ordinamento Giuridico Italiano e Dell'Unione Europea', *Rivista Amministrativa Della Repubblica Italiana*, no. 5–6 (2015): 227.

<sup>415</sup> See Legislative Decree 61/2011 article 2 (b): [personal translation] "infrastructure: an element, system or part thereof, which contributes to the maintenance of the functions of society, health, safety and economic and social well-being of the population".



national contact point. As permitted by the Directive, an additional supporting authority is designated as the “responsible structure”. Although the name may be misleading, this is simply a structure within the Prime Minister's Office that is tasked with technical and scientific activities related to the identification of ECIs. It is designated by a Prime Ministerial Decree<sup>416</sup>.

As mentioned in the European Policy Review, the work of the European Programme for Critical Infrastructure Protection had continued with the proposal to establish a Critical Infrastructure Warning Information Network (CIWIN). The subject was subject to a patchwork of protective measures and obligations, with a total lack of horizontal minimum standards. Facilitating the exchange of information between Member States was a complex task that required a well-planned approach, especially given the sensitive nature of the information<sup>417</sup>.

The issue of critical infrastructure had remained crucial even after the entry into force of the Directive, as confirmed also by the Stockholm Strategy and the new European Strategy for Internal Security. Both communications stressed the importance of improving the protection of infrastructures, both to reduce their vulnerability to attack and to better combat cybercrime<sup>418</sup>. To this end, they stressed the urgency of analysing and revising the Directive, only a few years after its entry into force. According to Article 11 of the Directive, a specific review should have taken place in 2012<sup>419</sup>.

The results of the initial analysis revealed a number of shortcomings, unfortunately inherent in the general regulatory framework, which proved to be too permissive. By 2012, most Member States had implemented the provisions, many of which did not even consider legislative changes necessary as similar obligations already existed in their national legislation.

Several observations can be made following the various stages of the identification process of European Critical Infrastructures.

With regard to identification, most countries had applied the sectoral criteria with only a few adjustments to adapt them to the existing national approach. The reason for the significant difference in the number of identified European Critical Infrastructures between the different sectors lies in this approach. In fact, almost all Member States started the identification process with a known list of national critical infrastructures, which was considered to be the entire starting point for the search for critical infrastructures of European relevance<sup>420</sup>. In this way, by starting from the list of national operators and

---

<sup>416</sup> See D.P.C.M. of 17 May 2011, designating the “Segreteria Infrastrutture Critiche” (SIC), existing within the Office of the Military Adviser of the Presidency of the Council of Ministers.

<sup>417</sup> European Commission, Proposal for a Council Decision on a Critical Infrastructure Warning Information Network (CIWIN) {SEC(2008)2701} {SEC(2008)2702}, 2–3.

<sup>418</sup> Council of the European Union, Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, 25; European Commission, ‘The EU Internal Security Strategy in Action’, 2.

<sup>419</sup> Many of the considerations that follow are drawn from this European Commission working paper, which you are invited to consult for further details. European Commission. See European Commission, ‘Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCIP)’, 22 June 2012, 5–14, SWD(2012) 190 final, [https://home-affairs.ec.europa.eu/system/files/2020-09/epcip\\_swd\\_2012\\_190\\_final.pdf](https://home-affairs.ec.europa.eu/system/files/2020-09/epcip_swd_2012_190_final.pdf).

<sup>420</sup> Member States had adopted different identification mechanisms, some simply using their own list of national critical actors, others using a bottom-up identification method by requiring an identification report to be sent to the competent authority. Although in many cases the criteria and definitions of the Directive have been transposed without significant variations, there are still very different national interpretations, some of which have not been made public, due to their sensitive nature. Further information can be found at 5.3

gradually subtracting from it, there was a risk of omitting many European critical infrastructures that were not relevant at national level. Similarly, the impact of nationally irrelevant critical infrastructure on other Member States had not been properly assessed.

With regard to the designation of European Critical Infrastructures, the process had been carried out through bilateral discussions between Member States, which might be suitable for smaller infrastructures, but not for larger ones across Europe. Consequently, Italy, together with other Member States, had stressed the need for multilateral discussions, especially given the natural extension of sectors such as energy and transport. In short, in the case of a critical infrastructure that crosses several Member States, it could be considered relevant at European level in the section between some of them, without guaranteeing the same level of protection for its entire extent.



Figure 10 - Concept of European Critical Infrastructure between different European countries

Consider, for example, a transport infrastructure running through France, Italy and Austria. Its designation as a European Critical Infrastructure would require two bilateral dialogues, one between France and Italy and the other between Italy and Austria. As a result, four different scenarios could arise: a) the CI is considered to be ECI for its entire length; b) the CI is not considered to be ECI for its entire length; c) the CI is considered to be ECI only for the section between France and Italy; d) the CI is considered to be ECI only for the section between Italy and Austria. Although this is a simplified example, far more complex situations involving relations between more than three countries could arise<sup>421</sup>.

---

Identification of ECI. See European Commission, 'Evaluation Study of Council Directive 2008/114 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection', 2 April 2019, 17–19, <https://op.europa.eu/en/publication-detail/-/publication/118dcd3d-b041-11ea-bb7a-01aa75ed71a1#>.

<sup>421</sup> Although this designation process was crucial to the overall design of the Directive, it was not overly

Despite the difficulties of comparison with the previous scenario, due to the lack of studies and the variety of regulations normally applicable to the different operators, it is nevertheless possible to attempt a general assessment of the impact of the Directive. The report noted that the effects varied according to the level of progress of the Member State in the field of critical infrastructure. The most advanced countries in the sector had not perceived much added value, while comparatively less mature states had attributed great results to the programme. Certainly, looking at the results, very few European Critical Infrastructures were actually highlighted, so that the comprehensiveness of the coverage of the legal framework can be questioned. However, the legislation has certainly contributed to a general increase in awareness and the level of cooperation in the European Union on critical infrastructure.

In terms of harmonisation effect, there were still rather large gaps between the different Member States. The definitions themselves have been transposed with a certain degree of heterogeneity, in particular as regards the nature of critical infrastructure, an aspect closely linked to the perception of national security. Therefore, “there is a potential tension between the EU definition of CI and that of the Member States” due to “the degree of sophistication of national CIP strategies and their respective definitions vary”<sup>422</sup>.

Contrary to expectations, “the current view of CIP in the EU emphasises the protection of infrastructures and prevention of disturbances, such as disasters, and relatively little attention is paid to recovering from disasters”<sup>423</sup>. The focus should be shifted from the concept of security measures to that of infrastructure resilience, which has instead remained a purely academic debate, despite the significant economic benefits. It is far better to focus on the ability of a system to continue to operate and return to normal in the event of an incident, since total protection can never be achieved.

As a more recent report on the Directive points out<sup>424</sup>, it is only partially relevant today, although its objectives are certainly still relevant. “The increased interconnectedness of and interdependencies between sectors, and the transboundary nature of threats and the potential consequences of the disruption/destruction of CI illustrates the continued need for the EU to be involved in this policy area”<sup>425</sup>. It is precisely the increased importance of these interrelationships that does not allow a generalised approach to risk to be fully pursued, in particular because of the limited scope of regulation. Its overall framework seems better suited to dealing with more traditional risks than those arising in a digital society.

From the point of view of coherence with other European legislation, there does not seem to be any particular conflict or synergy. In the uncertainty between overlap and mutual reinforcement, the prevailing view is that there is still a lot of potential to be exploited due to the lack of coordination.

In terms of effectiveness, however, it can be said that the Directive has achieved its promised objectives, albeit partially. In short, a common framework for the identification of

---

formalised due to the sensitive nature of the information. European Commission, 19–21.

<sup>422</sup> Pursiainen, ‘The Challenges for European Critical Infrastructure Protection’, 725.

<sup>423</sup> Pursiainen, 727.

<sup>424</sup> The following comments are drawn mainly from the following report, which you are invited to refer to for further consideration. See European Commission, ‘Evaluation Study of Council Directive 2008/114 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection’, 67.

<sup>425</sup> European Commission, 67.

European Critical Infrastructures has been put in place, as well as a common approach to risk assessment and some minimum procedures for coordination at both national and European level. Admittedly, the number of identified infrastructures is small and the procedures are not uniformly applied, but there are also clear positive externalities. Just think of the high level of awareness and the renewed political momentum around the issue of critical infrastructure, especially in those states that did not have a developed national framework. The Directive has paved the way for the introduction of a Europe-wide framework, including a common vocabulary. Several effects will continue over time, even without further action.

Unfortunately, however, this consideration only applied outside the Italian scenario, where critical infrastructures still suffered from an apparent regulatory vacuum, despite multiple sources of regulation. Even after the transposition of the Directive, there was still no legal definition of national critical infrastructure and no measures had been taken to secure it. There was a clear problem in identifying the country's critical interests<sup>426</sup>.

Immediately following the review of the Directive's impact, the European Commission launched a new approach to critical infrastructure, taking into account their cross-border interconnection. "The review process of the current EPCIP, conducted in close cooperation with the Member States and other stakeholders, revealed that there has not been enough consideration of the links between critical infrastructures in different sectors, nor indeed across national boundaries"<sup>427</sup>. The proposal was to work on the identification of four critical infrastructures with a European dimension<sup>428</sup> in a pilot phase and to give more management powers to the Commission in order to improve accident prevention, preparedness and response.

Since then, the issue of resilience has remained at the heart of EU policy, as evidenced by the new Internal Security Strategy in and the new Global Strategy in 2016. The 2017 Comprehensive Assessment of EU Security Policy highlights "the need for wider consideration of the implications that new security challenges and increased interdependency between infrastructures might have going forward called for a review of the Directive considering the need to repeal"<sup>429</sup>. As this chapter shows, especially in its introduction, only a few years after its revision, the CI Directive is only one piece of a larger picture, but a fundamental one.

The urgency of action was echoed by the European Parliament, which stressed the importance of protecting infrastructure from cyber-attacks by reducing inherent vulnerabilities. This would be the most effective way to continue the fight against cybercrime, which could not only consider repressive measures<sup>430</sup>. It was also unanimously endorsed by

---

<sup>426</sup> Luisa Franchina, 'Le Infrastrutture Critiche e La Protezione Cibernetica Nazionale', *Gnosis*, no. 4 (2013): 106–7.

<sup>427</sup> European Commission, 'COMMISSION STAFF WORKING DOCUMENT on a New Approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures More Secure', 28 August 2013, 3, [https://home-affairs.ec.europa.eu/system/files/2020-09/swd\\_2013\\_318\\_on\\_epcip\\_en.pdf](https://home-affairs.ec.europa.eu/system/files/2020-09/swd_2013_318_on_epcip_en.pdf).

<sup>428</sup> The four infrastructures were Eurocontrol, Galileo, the electricity transmission system and the gas transmission system.

<sup>429</sup> European Commission, 'Evaluation Study of Council Directive 2008/114 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection', 7.

<sup>430</sup> European Parliament, 'European Parliament Resolution of 3 October 2017 on the Fight against Cybercrime (2017/2068(INI))', 3 October 2017, 9, [https://www.europarl.europa.eu/doceo/document/TA-8-2017-0366\\_EN.pdf](https://www.europarl.europa.eu/doceo/document/TA-8-2017-0366_EN.pdf).

the Council of the European Union in its conclusions of 10 December<sup>431</sup>. It was in this context that the Commission presented its proposal for a new directive on critical infrastructure, the procedure for which was recently completed in December.

### *III.1.3.3 The new European Critical Infrastructures directive*

“The proposal on critical entities itself reflects a switch from the current approach focusing on the protection of individual assets towards strengthening the resilience of the critical entities that operate them. While the all-hazards approach of the existing directive remains valid, the new proposal embraces today's complex realities”<sup>432</sup>, both by extending the scope and by giving the Commission specific oversight of critical facilities of particular European importance.

The recitals of the new Directive begin by acknowledging precisely these contingencies, which called for an urgent replacement of the previous regulatory framework. Although “critical entities, as providers of essential services, play an indispensable role in the maintenance of vital societal functions or economic activities in the internal market [...] the evaluation of Directive 2008/114/EC conducted in 2019 found that, due to the increasingly interconnected and cross-border nature of operations using critical infrastructure, protective measures relating to individual assets alone are insufficient to prevent all disruptions from taking place”<sup>433</sup>.

The first observation to be made is that, a decade on, the legislation still focuses on the single market, using the powers typical of the first pillar<sup>434</sup>.

This is clearly reflected in its scope, which provides for the application of specific measures for the maintenance of services essential for the continuation of economic or social activities. Although this was also an objective of the previous Directive, it was not explicitly formulated, but remained an indirect objective of the efforts to achieve greater resilience of infrastructure. However, resilience remains the key theme, which is broken down and specified according to the main contents of the Directive: the introduction of obligations for critical facilities to improve their resilience, the introduction of rules for their identification and control, the establishment of common procedures for cooperation and reporting, and measures to achieve a high level of resilience<sup>435</sup>.

The decisive extension of the scope, previously limited to the energy and transport sectors, can be seen in the combination of Article 1 and the Annex. From the initial two, there are now 11, with perfect alignment with the NIS2 Directive. The most important additions are the financial and banking sector, digital infrastructure, public administration and, albeit with some clarifications, space.

---

<sup>431</sup> Council of the European Union, ‘Complementary Efforts to Enhance Resilience and Counter Hybrid Threats - Council Conclusions (10 December 2019)’, 10 December 2019, 7, <https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/en/pdf>.

<sup>432</sup> Irmgard Anglmayer, ‘European Critical Infrastructure - Revision of Directive 2008/114/EC’, Briefing (European Parliamentary Research Service, February 2021), 11, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662604/EPRS\\_BRI\(2021\)662604\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662604/EPRS_BRI(2021)662604_EN.pdf).

<sup>433</sup> See recitals 1 and 2 of directive (EU) 2022/2557.

<sup>434</sup> Whereas the first directive was based on Article 308 of the Treaty on the European Community, the new legislation is based on Article 114 of the Treaty on the Functioning of the European Union.

<sup>435</sup> See article 1 of directive (EU) 2022/2557.

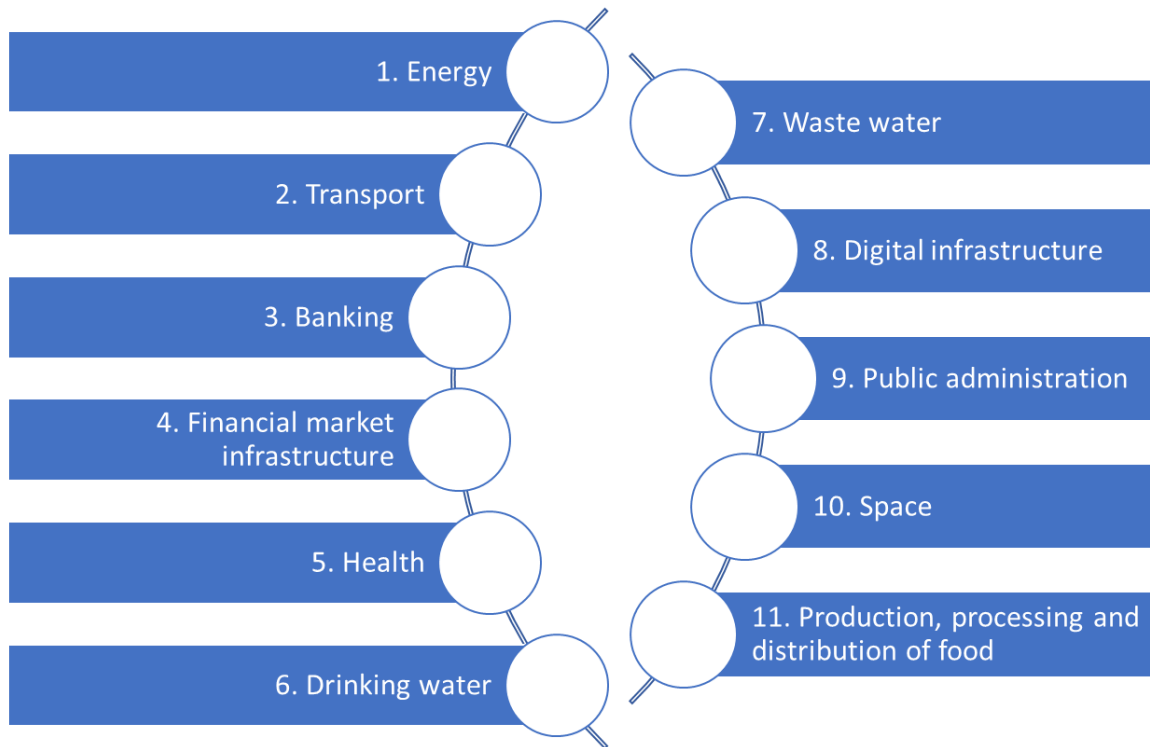


Figure 11 - European Critical Infrastructures' sectors

The scope also reflects the European legislator's great efforts to coordinate with other legislation. On the one hand, the intention is not to encroach on the competence of individual Member States in matters of national security and defence. On the other hand, the intention is to avoid an excessive administrative burden resulting from the unnecessary duplication of several pieces of legislation dealing with resilience, a concept that is generally transversal and dealt with at different levels. Accordingly, Member States are urged to achieve resilience as a result, without imposing rigid mechanisms or procedures. Where this objective is achieved by national provisions deemed equivalent, the Directive need not apply. While the Directive leaves the assessment of national legislation to each Member State, the European legislator explicitly exempts the application of critical infrastructure legislation where it overlaps with the new cybersecurity legislation, which is also being replaced in parallel<sup>436</sup>. The fact that the revision of the two subjects took place in parallel helped to improve co-ordination, which also led to greater clarity in the provisions.

Greater clarity can certainly also be seen in the wording of the definitions, which move away from the strict individual infrastructure asset approach. The concept of Critical Infrastructure is complemented by that of Critical Entity, which conceptually encompasses all the different assets for the proper maintenance of an essential service. It is no coincidence that the two definitions are listed one after the other, followed by the definition of an essential service<sup>437</sup>.

<sup>436</sup> See paragraph III.2.2.

<sup>437</sup> For the sake of simplicity, I will list the definitions below:

“‘critical entity’ means a public or private entity which has been identified by a Member State in accordance with Article 6 as belonging to one of the categories set out in the third column of the table in the Annex”;

Greater generality is favoured, which is later compensated by greater precision in the procedures. The Annex itself has also been made more detailed, since the breakdown into sectors and subsectors has been supplemented by the identification of certain categories of subjects, to limit the discretion of each Member State as much as possible. The need for flexibility and constant updating is met by granting the European Commission delegated standardisation powers to draw up delegated acts, which are useful for specifying typified concepts. This also demonstrates the active coordination role that central institutions should play<sup>438</sup>.

The review of the legislation is grouped into chapters, which makes it possible to identify the focal points worthy of attention, as well as the main differences following repeal. Four relevant blocks can be identified.

First, as in the previous legislation, obligations are defined both for individual Member States and for what are now defined as critical entities<sup>439</sup>. States are still obliged to designate competent authorities and a contact point to ensure more effective cooperation. In addition, the supervisory activities of national authorities, which should be able to impose appropriate sanctions in the event of non-compliance, are better specified<sup>440</sup>. Their activities will be complemented by the establishment of a specific coordination body, the Critical Entity Resilience Group, composed of representatives of the Member States and chaired by the Commission. This body should facilitate co-operation and information exchange through regular meetings, also jointly with the new NIS2 Co-operation Group. On the other hand, critical facilities remain obliged to designate a contact person for the national authority and to take risk-appropriate technical and organisational measures, described in a resilience plan. Finally, the section devoted to critical facilities of European importance, which has hitherto existed separately from the regulations, is completely new, following the introduction of a pilot phase of experimentation from the first evaluation of the Directive<sup>441</sup>.

Looking more specifically at Member States' obligations, it is worth noting the preparation of a strategy at national level to improve the resilience of critical facilities, which certainly draws on the experience of the first NIS Directive, which had ushered in the era of national cyber security strategies<sup>442</sup>.

The key issue remains the identification of critical entities, which follows a very detailed

---

“‘critical infrastructure’ means an asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, which is necessary for the provision of an essential service”;

“‘essential service’ means a service which is crucial for the maintenance of vital societal functions, economic activities, public health and safety, or the environment”.

Given the lack of clarity of the concept of public administration, a specific definition is also introduced, together with some criteria for distinguishing the public sector for the purposes of applying the legislation.

<sup>438</sup> See articles 23 and 24 of directive (EU) 2022/2557. When adopting delegated acts, the Commission must first consult the experts appointed by each Member State and inform both the European Parliament and the Council of the European Union, which have a right of veto. The possibility of adopting delegated acts could, for example, be used to identify new essential services within the scope. Compare article 5.

<sup>439</sup> See Chapters II and III of directive (EU) 2022/2557.

<sup>440</sup> See Chapter VI of directive (EU) 2022/2557.

<sup>441</sup> See Chapter IV of directive (EU) 2022/2557.

<sup>442</sup> Each Member State must adopt a strategy by 17 January 2026 and notify it to the Commission within three months of its adoption. See article 4 of directive (EU) 2022/2557.

procedure<sup>443</sup>. The first step is to carry out a sectoral risk analysis, based on the list of essential services established by the European Commission through a delegated act, considering all types of risks, including traditional ones. From the results of this analysis, it is then possible to identify the critical entities in each sub-sector which, by definition, are linked to the provision of essential services. The identification process involves the application of certain criteria: a) the entity must provide one or more essential services, b) it must operate on the territory of the Member State, and c) an incident affecting it should have a significant disruptive impact. Certain criteria for assessing the severity of the effects of the incident are also laid down, in a manner not dissimilar to the previous legislation. In order to avoid a heterogeneous approach to their application, in particular because of the sensitivity of the underlying reasoning, which also concerns national security, the Commission is assigned the task of developing guidelines for this identification phase.

Once the various critical facilities have been identified, a complete list with all critical entities must be drawn up. They must be notified of their designation within one month and informed of their obligations under the Regulations, with particular attention to the need for coordination with other EU legislation. This is not only about cybersecurity, i.e. the NIS2 Directive, but also about the banking sector and the financial market, for which there are already specific obligations regarding resilience and security measures<sup>444</sup>. Unless Member States decide otherwise, most of the legislation will not apply to these sectors to avoid unnecessary duplication. The same applies to the designation of competent authorities, which must cooperate without overlapping with those established under other legislation.

The list must be updated at least every four years and shared with both the NIS authorities and the European Commission<sup>445</sup>. In general, the legislation aims to promote horizontal cooperation between the different national authorities and between the different Member States, as well as vertical cooperation with the European institutions.

With regard to the obligations incumbent on the various critical entities once they have been designated, the obligation to adopt appropriate security measures has already been mentioned. Again, the starting point is a risk assessment that each entity must carry out within nine months of receiving notification of its designation and update at least every four years. This should be based on the results of the national risk assessment. The security measures are not listed in a typical or exhaustive manner, but certain purposes are presented that they must serve<sup>446</sup>. This includes ensuring adequate security in personnel management, which can be achieved through background checks. This possibility is a novelty introduced by the legislation, which aims to facilitate the verification of the identity and criminal record of personnel performing sensitive functions. As in the first Directive, Member States are encouraged to make use, where appropriate, of the newly introduced European standardisation in the field of cybersecurity<sup>447</sup>.

In order to avoid heterogeneous approaches, not only is the Commission given the task of

---

<sup>443</sup> See articles 5, 6, and 7 of directive (EU) 2022/2557.

<sup>444</sup> See article 8 of directive (EU) 2022/2557.

<sup>445</sup> Other information must also be provided to the Commission, such as the list of essential services identified in the national territory and the thresholds used to specify the criteria for defining significant disruption. See article 7 of directive (EU) 2022/2557.

<sup>446</sup> See article 13 of directive (EU) 2022/2557.

<sup>447</sup> See article 17 of directive (EU) 2022/2557.



developing guidelines, but Member States are also given the option of requesting an advisory mission from the Commission and its experts in order to better fulfil their obligations under the legislation<sup>448</sup>.

Another new aspect is the obligation to notify the supervisory authority of incidents that may have a significant impact on the essential service, in a manner similar to NIS and other regulations. The notification must be made within 24 hours of knowledge of the incident and must be followed by a more detailed report within one month, indicating the number of users affected, the time taken to recover from the incident and the geographical area affected. If an incident could have a significant impact on the continuity of provision of an essential service in six or more Member States, the competent authority must in turn notify the European Commission.

A final comment concerns critical facilities of particular European importance. The European legislator wanted to include this now unavoidable issue in the legislation, following the success of the introduction of this new comma approach, which had been tested in advance on a small circle of typical infrastructures<sup>449</sup>. Criteria have therefore been established to identify these special entities. First, they must be critical entities providing essential services to or in six or more Member States. This characteristic must be declared by the entity itself upon receipt of the notification of identification as “critical”, so that the national authority can inform the Commission, which must then consult all interested parties<sup>450</sup>. If the outcome of the consultations is positive, the entity will be informed of its new status and the resulting obligations through the national authority. Again, advisory missions from the European Commission are possible.

Finally, it should be pointed out that this is only a brief commentary on the new regulatory framework, which must be transposed by the Member States by 17 October 2024. It is certainly too early to assess the smooth functioning of the provisions, which will also have to be assessed in the light of the enforcement practices and methodologies that will be developed, also thanks to the delegated acts of the Commission.

A first objective assessment of implementation by the Commission is scheduled for 17 July 2027, while an assessment of effectiveness will have to wait until 17 June 2029.

The only certainty at this stage is that the adoption of the new directive comes at a time of great concern for critical infrastructure, only a few months after the Nordstream pipeline disaster, which was strongly condemned by the Council of the European Union<sup>451</sup>.

### III.2 The NIS Framework

After all the space devoted to what is defined as cybersecurity-related regulation, it is only natural that the section devoted to regulation strictly related to cybersecurity should begin with a discussion of the NIS system, which constitutes the core of the European protection

---

<sup>448</sup> See article 13 of directive (EU) 2022/2557.

<sup>449</sup> See footnote 428.

<sup>450</sup> The individual critical entity, the national authority that identified it and the national authorities of all the Member States in which essential services are provided by that entity must be consulted. See article 17 of directive (EU) 2022/2557.

<sup>451</sup> Council of the European Union, ‘Council Recommendation of 8 December 2022 on a Union-Wide Coordinated Approach to Strengthen the Resilience of Critical Infrastructure (Text with EEA Relevance) 2023/C 20/01’, 20 January 2023, 2, 2023/C 20/01, <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32023H0120%2801%29>.

system and the cornerstone of all subsequent interventions.

As was recognised in the introduction to this chapter, the interventions most relevant to the sector have a relatively recent history, limited to the last decade. On the other hand, where the problem has been dealt with indirectly, as an appendix to others, the examination requires more in-depth analysis, since the last thirty years have to be covered.

Despite the reduced availability of consolidated studies and debates, the issue is no less relevant. On the contrary, the regulatory system, which will be implemented by the end of 2024 after the reform, requires a thorough analysis to understand how it works. First and foremost, the context of the introduction of the first NIS Directive deserves to be addressed.

The attempt to reconstruct an essential chronology of the security of information systems is inevitably intertwined with various non-binding interventions, as highlighted in the first chapter. Although the subject was not always exclusive, it is possible to trace its origins well before the first proposal for a directive on the subject. The first document to use the terms network and information security was a 2001 Communication from the European Commission, which attempted to lay the foundations for a first regulatory approach. The complexity behind this effort was recognised and network and information security was for the first time outlined as an autonomous and partially overlapping area with other policy areas, such as the fight against cybercrime, the protection of personal data and electronic communications. Network and information security was defined as "the ability of a network or an information system to resist, with a given level of confidence, accidental events or malicious actions"<sup>452</sup>.

Shortly afterwards, the definition would be taken up and clarified in the founding regulation of ENISA, which would lend itself to important definitional work that would lay the foundations for a first common lexicon at European level. Certainly, the creation of a specific agency was a further and obvious step forward in this field, albeit a temporary one without any real operational powers.

The natural next step can be seen in the so-called Strategy for a Secure Information Society, which can be seen as an extension and completion of the initial ideas put forward by the Commission in 2001. As the initial efforts began to lose momentum, the Commission stepped in again to review progress and reinforce a holistic, multi-stakeholder approach. In doing so, it would also have hoped for coordination in the area of critical infrastructure policies, which are largely overlapping due to their increasing degree of digitalisation. As analysed in more detail in the dedicated section, it was precisely during these years that the European Programme for Critical Infrastructure Protection (CIP) was launched, and one of its main outcomes was the first CIP Directive.

Together with the regulation establishing ENISA, which was later reformed in 2013, and the telecoms reform that came into force in 2009<sup>453</sup>, this would have been one of the few binding measures related to information security. This would be followed by non-binding

---

<sup>452</sup> European Commission, 'Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach', 3. the Green paper identified three types of infrastructures assets: public, private and governmental infrastructure, procedures where relevant individuals that exert control over critical infrastructure function, and objects having cultural or political significance. In this way, "by focusing on the 'assets' provided by infrastructures, one can more adequately reach their socially and culturally underlying value". See Burgess, 'Social Values and Material Threat', 479.

<sup>453</sup> For more information about telecommunications, see paragraph III.1.1.

communications, which would further intertwine cybersecurity with the issue.

Not only the 2009 Communication on Critical Infrastructure Protection, but also the Tallinn European Council Conclusions had pointed out that the increase in cyber-attacks and incidents required an increased focus on infrastructure protection in a collaborative approach. Such an intervention was necessary in the face of heterogeneous and fragmented national approaches, which were not able to promote an adequate level of integration at both national and international level. As noted elsewhere, developments in this area would later lead to further clarifications that would form the basis of the first critical infrastructure review<sup>454</sup>. From an information security perspective, this was relevant given the tendency of many cyber security measures to protect infrastructure. The Commission itself called in vain for Member States to set up national CERTs quickly by the following year, but the situation of voluntary implementation was bound to continue with a significant delay.

While progress was made in the fight against cybercrime with the Directive on attacks against information systems and the establishment of the European Cybercrime Centre, there was no positive outcome in terms of the overall level of protection of information systems.

This was despite the fact that the issue was a key policy in the Union's new 'Europe 2020' political strategy, which devoted a special place to the Digital Agenda.

Work on a proposal specifically dedicated to cybersecurity began in 2013, and would lead to the adoption of the famous NIS Directive and its effectiveness in August 2016. The impact assessment accompanying the proposal further highlighted the ineffectiveness of the legislation in force at the time. Although minimal, some IT security obligations existed for operators and could be derived from other disciplines.

Building on the above-mentioned regulations, the Critical Infrastructure Directive, although limited to the energy and transport sectors, required the establishment of a security plan describing the security measures taken as a result of a prior risk analysis.

Following the reform of the telecommunications sector, operators of telecommunications networks and services were required not only to take security measures to minimise the impact of incidents on users, but also to notify the authority of any breach of security or loss of integrity<sup>455</sup>.

The Directive on attacks against information systems, on the other hand, focused mainly on the pursuit of criminal policy through the criminalisation of specific conduct. As a result, it did not impose any particular additional obligations on operators in relation to their cybersecurity, at least not different from those generally adopted for the better prosecution of cybercrime.

Finally, some additional obligations were largely derived from the Data Protection Directive, which has been replaced by the new European Data Protection Regulation since May 2018. Despite this replacement, it can be said that the structure of the Directive was generally similar to the current one. Data controllers were required to implement technical and organisational security measures to protect personal data, taking into account the state of the art and the cost of implementation. The level of data protection should be

---

<sup>454</sup> European Commission, 'COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on Critical Information Infrastructure Protection "Achievements and next Steps: Towards Global Cyber-Security"'.

<sup>455</sup> As explained in the paragraph III.1.1, we refer here to the operators and providers of electronic communications services in the traditional sense. So-called over-the-top operators are excluded.

proportionate to the risk. This logic was later extended by the GDPR, which added the obligation to notify personal data breaches to the data protection authority. However, it should be stressed that the legislation only applied to the processing of personal data.

It can therefore be concluded that, prior to the NIS Directive, there was no legislation requiring companies to implement security measures and incident notification obligations where no personal data was involved, with the exception of the telecommunications sector.

Given the inadequacy of the above measures, it was not to be hoped that voluntary cooperation between Member States could be a viable alternative. Little cooperation was limited to a small circle of Member States that had independently achieved good preparedness in terms of cybersecurity, excluding the majority. On the other hand, the only fora where a dialogue on the issue could take place were either not specific or lacked real power to intervene. ENISA itself, which was recognised as having a crucial role to play in improving relations between Member States and with different stakeholders, was highlighted as being under-resourced<sup>456</sup>.

While all these considerations help to explain the need for harmonisation in this area, it is significant that the European legislator supported its choice of legal basis for the proposed directive<sup>457</sup>.

As in the case of many other interventions directly or indirectly related to cybersecurity, this basis is to be found in the specific possibility of adopting approximation measures for the creation and smooth functioning of the internal market<sup>458</sup>.

Initially, at least, this possibility was contested in several respects by the Member States, which had always been reluctant to cede competences to the European institutions, especially in horizontal areas that could affect their national interests. These conflicts have given rise to an interesting body of case-law of the Court of Justice of the European Union. Among the most interesting rulings are also situations directly related to ICT regulation.

One of the first cases concerned the legitimacy of the regulation establishing ENISA. On that occasion, the Court reaffirmed the breadth of the basis of Article 114 TFEU, which not only allows the legislator to adopt measures addressed to the Member States, but also allows a more general discretion as to the choice of methods of approximation of the various

---

<sup>456</sup> The European Commission stated that “the Agency’s activities appear insufficient to achieve the high level of impacts and value added hoped for, and its visibility is below expectations”. At the same time, however, ENISA importance “to enhance contacts and working relations with stakeholders and Member States centres of expertise”. See European Commission, ‘Communication from the Commission to the European Parliament and the Council on the Evaluation of the European Network and Information Security Agency (ENISA)’, 1 June 2007, 6–9, COM/2007/0285 final, <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52007DC0285>. Other relevant fora include European Forum for Member States (EFMS) and European Public-Private Partnership for Resilience (EP3R). The latter was set up to facilitate exchanges between Member States and ICT companies, although its non-binding nature in itself clashed with the reluctance of the private sector to make its security information public.

<sup>457</sup> European Commission, ‘COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the Document Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Level of Network and Information Security across the Union’, 7 February 2013, 31–32, SWD(2013) 32 final.

<sup>458</sup> Regardless of the changing references to the Treaties, which have undergone various modifications as a result of changing European balances, the basis of legitimacy is always the same. Take, for example, the regulation establishing ENISA, or the directives of the so-called telecoms package, which still referred to Article 95 TEC, later transposed into Article 114 TFEU.

national rules. This goes so far as to allow the creation of a Community body to contribute to the implementation of a harmonisation process, provided that it is given powers strictly related to the subject matter of the regulatory act<sup>459</sup>. The intervention was defined as appropriate to protect “the smooth functioning of the internal market” from the risk of “being undermined by a heterogeneous application of the technical requirements”<sup>460</sup>. In some respects, this decision represented both a strong awareness on the part of the European Court of Justice of the need to take action to harmonise the sectors affected by the wave of digitisation, but also an important authorisation for the European legislator to act with broad powers in this matter.

As a confirmation of the chosen regulatory basis, it is possible to report some elements that highlight the seriousness of a situation characterised by an insufficient level of protection against network and information system security incidents. This more general problem can be broken down into a number of more specific issues. On the one hand, “given that networks and information systems are interconnected and given the global nature of the Internet, many NIS incidents transcend national borders and undermine the functioning of the internal market”<sup>461</sup>. At the same time, if not properly managed, the situation would have risked worsening due to the “uncoordinated regulatory interventions [, which] may result in fragmentation and give rise to Internal market barriers generating compliance costs for companies operating in more than one Member States”<sup>462</sup>.

This interconnectedness, combined with a heterogeneous national approach, exacerbated the growing number of cyber incidents, which were not only quantifiable but also complex. This was compounded by the impossibility of obtaining comprehensive data due to the lack of an efficient reporting mechanism. The reluctance of victims to report prevented them from

---

<sup>459</sup> As this is not the place to enter into this jurisprudential debate, allow me to refer to a recent judgment which, through its references, makes it possible to reconstruct the principles of standardisation on the basis of Article 114 TFEU. First and foremost, “while a mere finding of disparities between national rules is not sufficient to justify recourse to Article 114 TFEU, it is otherwise where there are differences between the laws, regulations or administrative provisions of the Member States which are such as to obstruct the fundamental freedoms and thus have a direct effect on the functioning of the internal market”. This does not mean that this legal basis cannot be used as a preventive measure, but that it can only be used if the emergence of such obstacles is likely and the measure in question is designed to prevent them. This possibility is not hampered by previous interventions based on Article 114 TFEU, as the EU legislator can always intervene to “[adapt] that act to any change in circumstances or development of knowledge having regard to its task of safeguarding the general interests recognised by the Treaty”. “It is otherwise where there are differences between the laws, regulations or administrative provisions of the Member States which are such as to obstruct the fundamental freedoms and thus have a direct effect on the functioning of the internal market”. See *Czech Republic v European Parliament and Council of the European Union*, No. Case C-482/17 (ECJ 3 December 2019). In other words, the formula “approximate measures” contained in the provision, “intended to confer on the Community legislature a discretion, depending on the general context and the specific circumstances of the matter to be harmonised, as regards the harmonisation technique most appropriate for achieving the desired result, in particular in fields which are characterised by complex technical features”. *United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union*, No. Case C-66/04 (ECJ 6 December 2005).

<sup>460</sup> *United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union*, No. Case C-217/04 (ECJ 2 May 2006).

<sup>461</sup> European Commission, ‘COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the Document Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Level of Network and Information Security across the Union’, 12.

<sup>462</sup> European Commission, 13.

seeing the full picture, minimising the chances of an effective response<sup>463</sup>.

There was a directly proportional relationship between the economic benefits of digitalisation and the vulnerability of the various actors. Certainly, the introduction of ICT has had a positive impact on the economy, but in the long run, the inherent insecurity of the systems would have made it unsustainable to carry out any activity, especially for several sectors that are crucial for society<sup>464</sup>.

In summary, three main causes of the problem were identified. The first was the uneven cyber capabilities of Member States, which could be divided into groups according to their level of preparedness<sup>465</sup>.

The second and somewhat related issue was the adequacy of incident response capabilities, which were lacking in most Member States. Even where they did exist, different communication protocols persisted, making any exchange of information useless or extremely difficult. Indeed, the establishment of national CERTs was still at a very early stage<sup>466</sup>.

The third and final cause was therefore inadequate information sharing, driven by fear of potential reputational damage and a lack of adequate procedures for effective communication.

### III.2.1 The first NIS directive

Although the first directive has now been superseded by the latest amendment of December 2022, a careful examination of it is essential to understand the operation of the system on which the latest amendments will be grafted by October 2024.

Before getting to the heart of the analysis, I think it is worth highlighting a not insignificant aspect of the legislation under consideration, especially when compared to other parts of the so-called digital package. The NIS Directive makes no reference to fundamental rights. The only mention is in the last recital, which seems to play a mainly formal role, an obligatory reference to the Nice Charter, as if to fill the silence of the following provisions.

Cybersecurity does not confer rights on individuals, but is a matter of technical compliance. Indirectly, it could be said that an increased level of security could better guarantee the possibility of exercising other fundamental rights through digital means, but this is not an exact law. The conflicts between security and privacy highlighted above are evidence of the ambivalence that can arise and are nothing more than a technological deconstruction of the classic opposition between security and other fundamental rights of the individual.

In part, this necessary clarification seems to be in line with the objective of the legislation,

---

<sup>463</sup> European Commission, 13–15.

<sup>464</sup> As a result of the consultations, the following sectors were identified for partial inclusion in the first NIS Directive: a) energy, b) transport, c) banking and finance, d) health, e) internet services, and f) public administration.

<sup>465</sup> Apart from the strong preparedness of the Nordic countries and the United Kingdom, which were defined as 'champions', and some other countries following as 'pillars', well over half of the countries, including Italy, still had a lot to learn and catch up on, despite their good growth potential. See European Commission, 'COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the Document Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Level of Network and Information Security across the Union', 23.

<sup>466</sup> ENISA, 'National/Governmental CERTs ENISA's Recommendations on Baseline Capabilities', December 2014, <https://www.enisa.europa.eu/publications/national-governmental-certs-enisas-recommendations-on-baseline-capabilities/@@download/fullReport>.

which is to provide for measures to achieve a high and common level of security of networks and information systems within the Union in order to improve the functioning of the internal market<sup>467</sup>. This effort required both the introduction of new obligations and safeguards and the creation of new dedicated bodies. In addition, there has been a major effort to coordinate with other existing sector-specific legislation, which should not be affected by the application of this legislation<sup>468</sup>. Particularly noteworthy is the reference to data protection legislation, which seems to have been almost neglected, since, although its reform took place in parallel with that of the NIS Directive, reference was still made to the previous sources. This illustrates the lack of legislative coordination between the two processes and the missed opportunity to benefit from possible synergies<sup>469</sup>.

A further, albeit necessary, opening to fragmentation was the specification that each Member State was free to adopt measures for a higher level of safety. This gives an insight into the complexity of the system, which on the one hand allowed for the application of more specific sectoral rules at European level, but on the other hand left a great deal of freedom in implementation, even allowing for more obligations. However, given the different starting points of the Member States, it was understandable that the introduction of the Directive should not lead to a lowering of the level of protection offered by the more advanced countries in this field.

The core of the Directive revolves around the identification of two specific categories of recipients, operators of essential services and providers of digital services, to which Chapters IV and V respectively are devoted.

For the former, a more complex identification discipline is introduced, which can be found in Articles 5 and 6, which provide for a subsequent set of criteria and controls, not unlike the critical infrastructure legislation. The task of identification was assigned to the Member States, which had to implement it by 9 November 2018.

---

<sup>467</sup> See article 1 of the directive (EU) 2016/1148.

<sup>468</sup> Article 1 refers, on the one hand, to the obligations arising from the legislation on electronic communications and, on the other hand, to the obligations arising from the legislation on electronic signatures and trust systems (so-called eIDAS). In addition, reference was made to the legislation on critical infrastructures and to recent interventions in the field of criminal law.

<sup>469</sup> See article 2 of the directive (EU) 2016/1148.

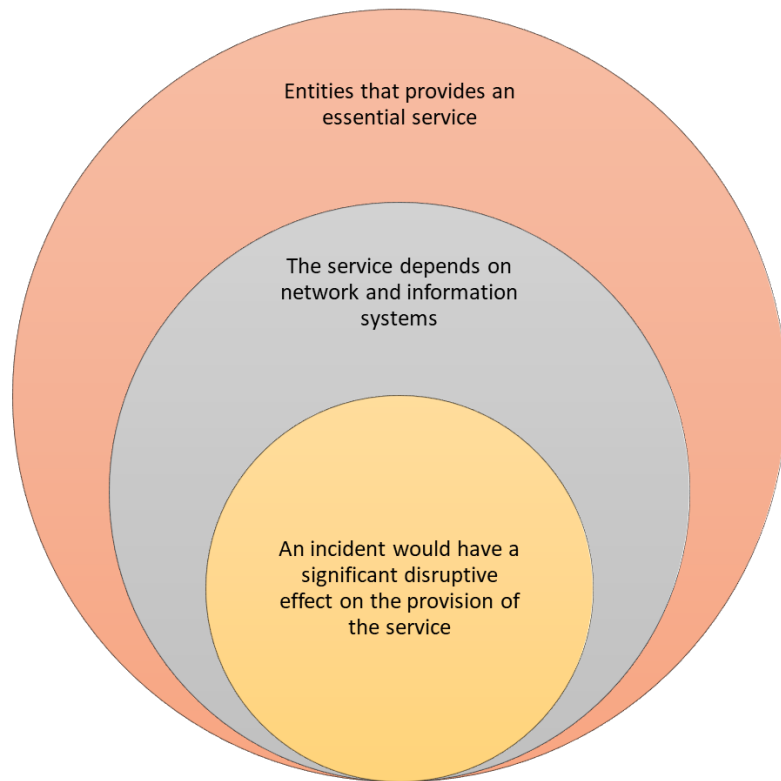
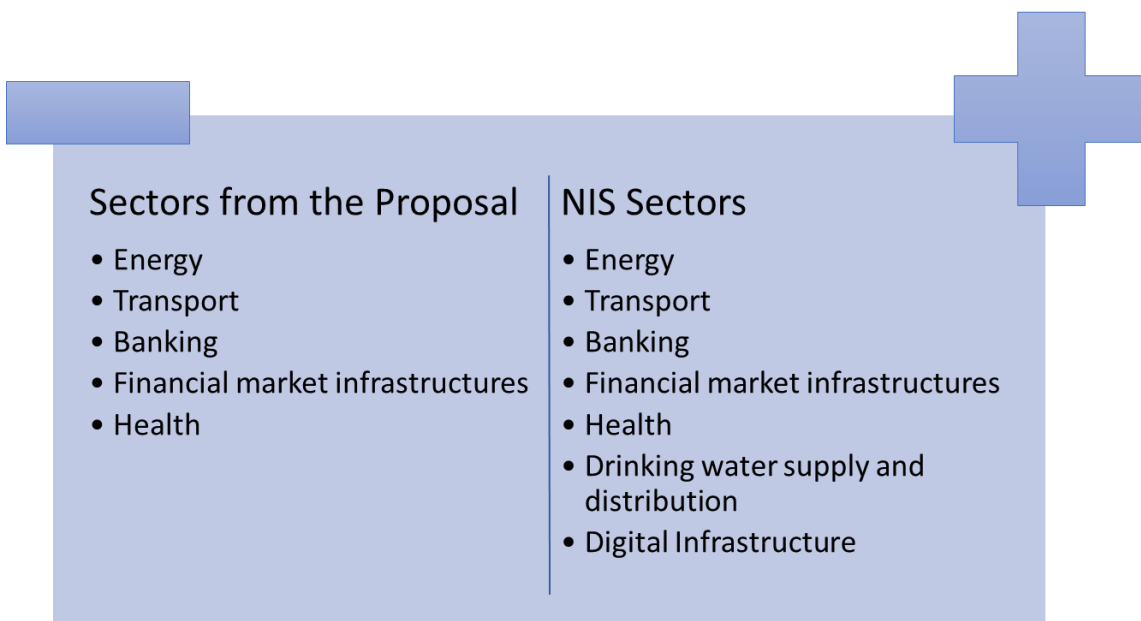


*Figure 12 - Scope of NIS1 Directive*

The diagram illustrates the logic of the various criteria to be applied progressively in order to identify the operators of essential services. In addition, as the definition in Article 2 makes clear, the Regulation does not cover all operators, but only those within a number of identified sectors listed in Annex II. As a result, not only are not all essential services affected, but even within the same sector there are significant exclusions, as can be seen from the different concentric circles. It is also worth looking at the sectors that have actually been regulated.





Although some additions to the original proposal can be noted, as shown in the figure, it should already be emphasised that several crucial sectors are missing, to which several Member States would have extended protection, at least at national level<sup>470</sup>.

Once the essential services in each sector had been identified, Member States had to apply the criteria sequentially, first by identifying the essential services that depend on networks and information systems, and finally by identifying where an incident would have a significant disruptive impact on their provision. The concept of significant adverse effects is further clarified in Article 6, which lists a number of criteria to be taken into account in the final step of the analysis<sup>471</sup>.

Where essential services are provided to two or more Member States, a consultation procedure between the different Member States concerned must be activated for the purposes of identification<sup>472</sup>. The results of the identification by sector must be updated at least every two years and compiled in a list to be communicated to the Commission every two years after the first deadline for identifying operators. The communication should be an opportunity to provide useful information for the revision of the Directive, such as the national rules introduced for identification or any thresholds introduced for the application

<sup>470</sup> This issue will be discussed in more detail in paragraph III.2.2.

<sup>471</sup> The criteria that must be taken into account are: a) the number of users relying on the service; b) the dependency of other sectors on that service; c) the impact that incidents could have, in terms of degree and duration; d) the market share of that entity; e) the geographic spread; f) the importance of the entity for maintaining a sufficient level of the service. In addition, sector-specific factors can be assessed.

<sup>472</sup> The consultation procedure was further specified in a reference document prepared by the NIS Co-operation Group. The process is divided into stages and the information to be transmitted is specified in detail. In part, the logic follows that of tacit consent, so as not to block discussions indefinitely. See NIS Cooperation Group, 'Identification of Operators of Essential Services Reference Document on Modalities of the Consultation Process in Cases with Cross-Border Impact - CG Publication 07/2018', July 2018, [https://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=53661](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53661).

of the criteria for assessing the relevant disturbance.

Once identified, operators of essential services must comply with a number of obligations. First, they must take technical and organisational security measures commensurate with the risk to the security of their networks and information systems, taking into account the state of the art. The aim must be to minimise the impact of incidents that could affect their security and thus the continuity of essential services. In order to ensure consistency, the NIS Cooperation Group has produced a Reference Document on Security Measures for Operators of Essential Services<sup>473</sup>.

The second relevant obligation is to notify the competent authority of all incidents that have a significant impact on the continuity of its essential services. It should be noted that the notification does not cover all incidents, but only those with a significant impact, which must be assessed on the basis of a number of criteria set out in Article 14(4) itself. Despite the existence of a set of readily applicable criteria, the assessment is only a seemingly straightforward process. As a study by the NIS Co-operation Group has shown: “The multitude of sectoral approaches mirrored the numerous discrepancies between types of OESs and the corresponding business models adopted, thus creating a deep pool of sometimes incompatible variables that must be taken into account when approaching such a regulation. [...] Achieving convergence between the myriad of existing approaches while sticking to the formal requirements might be troublesome”<sup>474</sup>.

---

<sup>473</sup> The document provides a comprehensive picture of the most common existing approaches in the Member States. It also identifies some general principles to guide the adoption of appropriate measures. Furthermore, the identified measures are described in four parts: governance and ecosystem, protection, defence and resilience, each of which is subdivided into more specific paragraphs. See NIS Cooperation Group, ‘Reference Document on Security Measures for Operators of Essential Services - CG Publication 01/2018’, February 2018, [https://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=53643](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53643).

<sup>474</sup> NIS Cooperation Group, ‘Reference Document on Incident Notification for Operators of Essential Services - Circumstances of Notification - CG Publication 02/2018’, February 2018, 24, [https://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=53644](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53644). The study shows how the practical application of even apparently simple criteria can give rise to insurmountable difficulties and lead to different practices at Member State level. Consider the number of users affected by an accident. This can easily be a number in all sectors where the business model involves the direct provision of services. This is not the case where the service is provided to an indeterminate number of people. Consider health care, where the “users” are not only the patients of a given facility, but potentially all individuals who may need health care services in a given area. If the operator of the essential service has knowledge only of its direct customers, but not of all its indirect customers, it would be counterproductive to ask it to process information that it cannot obtain, or that it could obtain only with considerable effort. Similar problems arise with the parameter of the duration of the incident, since the total period can be calculated from different points in time, depending on the choices made by the national legislator. Moreover, this parameter is not relevant in itself, but always requires another parameter, such as the number of users (an accident may last a long time but affect a small number of users). Geographical area, on the other hand, seems to be used only in part and only by sectors with a clear territorial scope. This is not the case for operators providing digital services to a wide audience. As a result, there are many different ways of applying the criterion in practice, leading to the need for a simple and unambiguous approach, which is still lacking. Although Article 14 (4) only mentions the three criteria just mentioned, it is clear from the document that this is not a typical set and that other useful criteria may be considered. For operators of essential services, it is suggested to use the criteria of Article 6, which are used for their identification, but may also be useful in the context of notification. The percentage of acceptance of all criteria is summarised in Figure 13. To make just a few more comments on the remaining criteria, it should be noted that the information required will require an appropriate set-up of the response system as a whole. For example, in order to know the interrelationships and dependencies between operators of essential services, each State will need to put in place mechanisms to identify them, either by forcing operators to cooperate or by cross-referencing reports of

### Adoption of the criteria by Member States

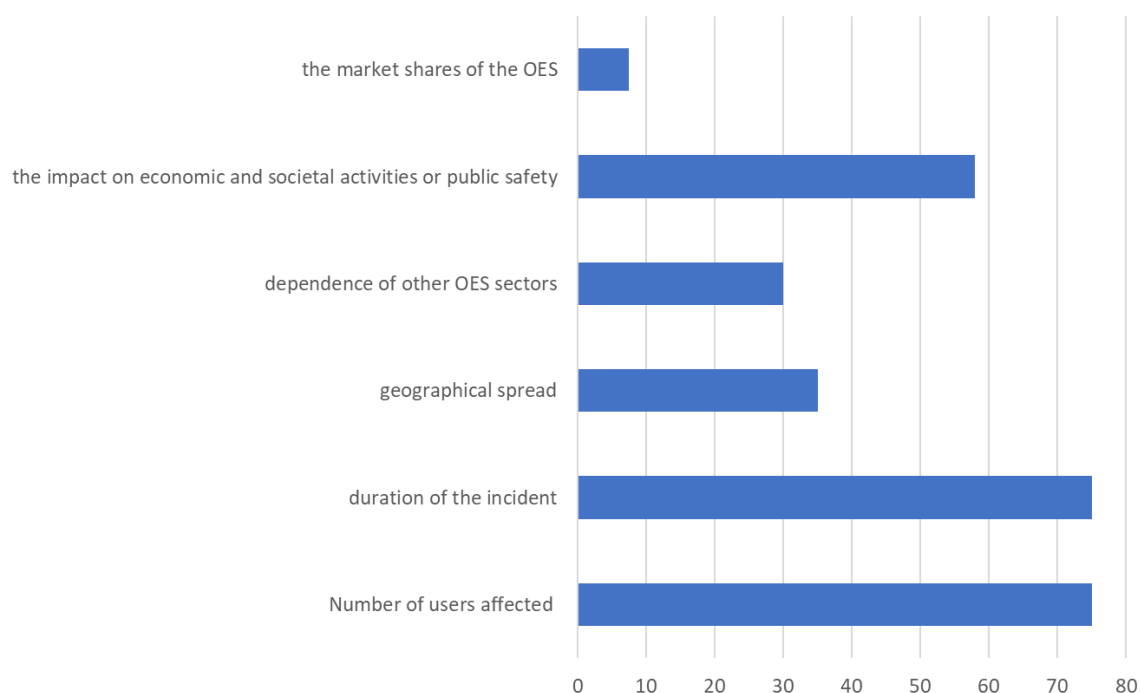
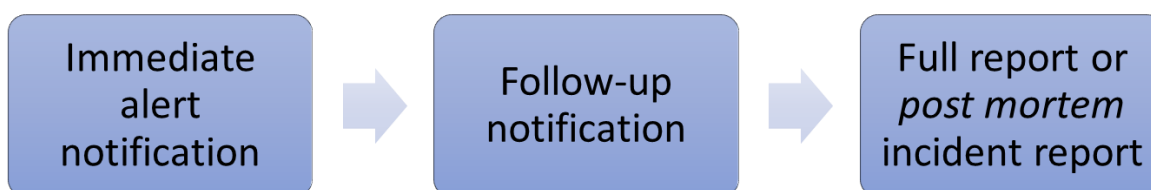


Figure 13 - Criteria to identify incidents' critical impact

Another aspect that should not be overlooked is the notification procedure to be followed. Under Article 14(7), guidelines can be drawn up through the Cooperation Group, which has issued some non-binding guidelines summarising and proceduralising the main obligations of the Directive. The first step is to identify the different moments of notification, which should not be seen as a point in time, but as a dynamic process in which an initial notification is followed by updates over time. Once the incident has been resolved, a comprehensive report is produced, recording all the updates<sup>475</sup>.



different incidents to trace the common root. Although economic impact is a widely accepted criterion, this requires knowledge of general data about society, as in the case of public safety, which are outside the normal activities of operators. Consequently, there is a high risk of error due to incomplete data. The market share criterion, on the other hand, is rarely used because there is no correct unit of measurement to interpret it. Although intuitively “the bigger the market share, the bigger the impact in case of an incident”, this measure does not immediately translate into useful data. See NIS Cooperation Group, 23.

<sup>475</sup> Each of these three phases, shown in the diagram, has its own specific function. While the initial alert is only intended to inform the authority and enable it to cooperate, the periodic updates are intended to update the scarce initial information and enrich it as the situation evolves. The final report, which is also known as the post-mortem report because it is submitted long after the rescue operation has been completed, is intended to provide a complete overview of the activities.

The Figure 15, on the other hand, shows how the notification has to be placed in a wider set of relationships, both between the different Member States and with authorities at European level. This also makes it possible to frame certain obligations on the part of the Member States, which are required to designate one or more competent authorities for the purposes of monitoring the NIS Regulation. However, where there are two or more authorities, only one of them can act as a contact point. The Commission must be notified of the designation and functions of the authorities, which must be provided with adequate resources and powers. In addition to the competent authorities, one or more CSIRTs must be established and tasked with handling incidents. To this end, they must be established with the characteristics set out in Annex I.

Having established this necessary premise, the relationships must then also include the new authorities established at European level, the so-called Cooperation Group and the network of CSIRTs. The role of the former is to support and facilitate strategic cooperation and exchange of information between Member States, which appoint representatives to it, together with the Commission and ENISA. One of its main tasks is to prepare an evaluation report on the experience gained in the field of NIS cybersecurity. The functioning of the Coordination Group is regulated by an implementing decision of the European Commission<sup>476</sup>. The second one unites officials from national CSIRTs and CERT-EU, who are responsible for technical and operational support in case of cyber incidents.

---

<sup>476</sup> European Commission, 'Commission Implementing Decision (EU) 2017/179 of 1 February 2017 Laying down Procedural Arrangements Necessary for the Functioning of the Cooperation Group Pursuant to Article 11(5) of the Directive (EU) 2016/1148 of the European Parliament and of the Council Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union', 2 February 2017, C/2017/0438, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017D0179>. The Regulation also specifies the elements to be taken into account when identifying measures to ensure the security of networks and information systems and when determining when an incident has a significant impact. First, Article 2 specifies the categories of security measures referred to in Article 16(1). Next, Articles 3 and 4 define the parameters for defining an incident as having a significant impact. In particular, thresholds are defined, such as the number of users affected per hour.]

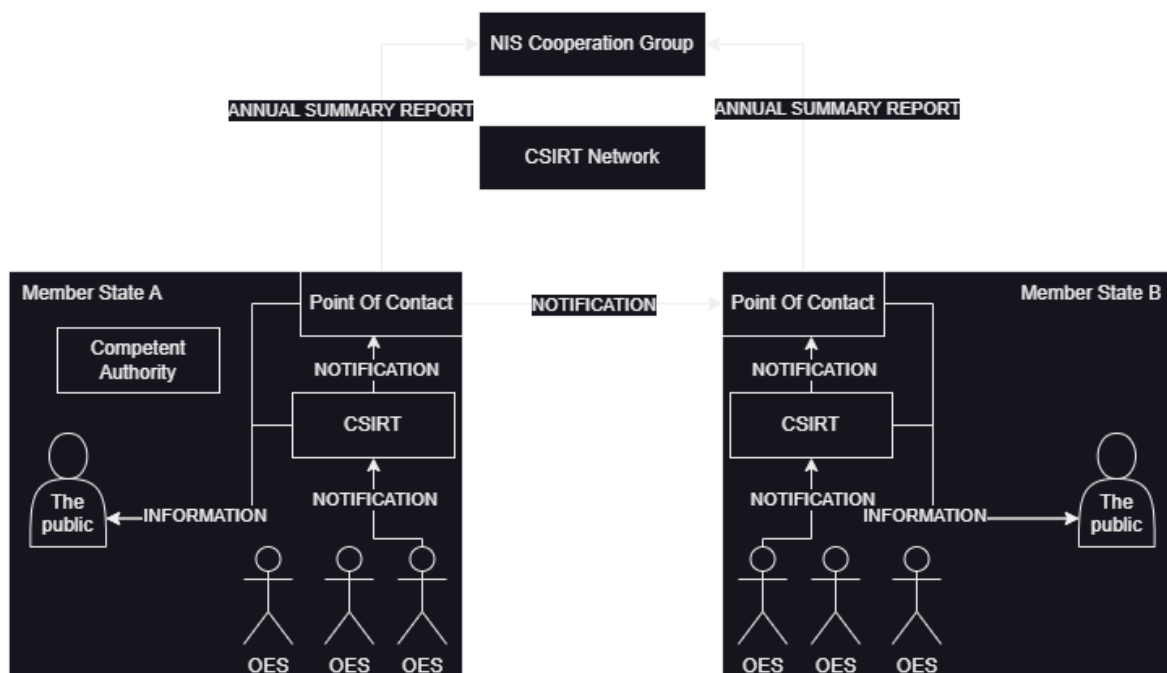


Figure 15 - NIS bodies in the NIS notification procedure

The diagram displays all of the entities mentioned earlier and illustrates the functioning of a notification process, which constitutes the initial step in a wider process. Considering that notification consists of numerous successive communications, as shown earlier, the affected essential services provider organizes the notification of the severe impact incident to either the competent authority or CSIRT. In the diagram, it is assumed that the notification is transmitted to the CSIRT if a country has designated numerous competent authorities and only one of them is considered the point of contact. When an incident has cross-border significance, the contact point ought to ensure that the notification is transferred to the contact point of the member country in question. The cooperation group should receive a summary report of incidents that have been notified to the competent authority or CSIRT on an annual basis. Upon consulting with the affected essential services operator, the CSIRT or competent authority must guarantee that the public receives timely notification about the incident. This takes place only if the operator has not already reported the incident, and if users outside the operator need to be informed.

The pertinent legislation regarding essential service providers concludes with equipping supervisory authorities with requisite powers and measures. The supervisory authorities shall be capable of soliciting the necessary information to evaluate network and information security, along with the evidence of the implementation of security policies. In the event of a failure, the supervisory authorities must provide mandatory instructions to operators for its rectification.

The remaining relevant regulation in the NIS area concerns digital service providers, for which a different logic has been adopted from that described for operators of essential services. Whereas the latter required sectoral identification, a comprehensive approach has been adopted for the former. In short, all digital service providers listed in Annex III are covered by the Regulation, so no identification procedure is required<sup>477</sup>.

<sup>477</sup> According to the Annex, digital service providers are online marketplaces, online search engines, and cloud computing services. See namely article 4 (17)(18)(19). On the other hand, the definition of a service can

Although the obligations are the same, namely the adoption of appropriate security measures and the notification of incidents, a combined reading with the recitals reveals the more permissive approach towards digital service providers. The European legislator recognises their “crucial importance for the smooth functioning of businesses that depend on them”<sup>478</sup>, as well the need to adopt a level of security commensurate with the degree of risk, but an implicit hierarchy is introduced between operators of essential services and providers of digital services. “In practice, the degree of risk for operators of essential services, which are often essential for the maintenance of critical societal and economic activities, is higher than for digital service providers. Therefore, the security requirements for digital service providers should be lighter. Digital service providers should remain free to take measures they consider appropriate to manage the risks posed to the security of their network and information systems”<sup>479</sup>.

Consequently, the fact that Article 16 specifies the elements to be taken into account for the adoption of specific security measures by digital service providers does not mean that these entities are subject to greater obligations. On the contrary, the list must be seen as a kind of guideline, precisely because of the greater freedom granted by the legislator. However, despite this greater freedom, the ubiquity and spread of these operators require a greater degree of harmonisation. This is why the Commission is given the task of intervening with delegated acts, both for safety measures and for the accident notification procedure<sup>480</sup>.

With regard to the notification of incidents, it is immediately apparent that the assessment criteria set out in Article 16(4) are more numerous than those for operators of essential services. In reality, however, the difference is only apparent because, as mentioned above, the guidelines of the cooperation group had called for the same additional criteria to be applied to operators of essential services. What is certain is that in this case the list of requirements cannot be extended because Article 16(10) prohibits Member States from imposing additional requirements on digital service providers. As if that were not enough, notification is only required if the provider has access to the information necessary to assess the impact of the incident, unless it is delegated to the operators of essential services on which they depend<sup>481</sup>. This should be enough to show how lax the obligations are for digital service providers.

In short, it is possible to confirm that the obligations are not different, there is a different level of enforcement. This can also be seen in terms of the supervision of the supervisory authorities, which are only required to intervene ex post, where there is “evidence that a

---

be found in Article 1(1) of Directive 2015/1535: ‘Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services’. According to this, the service in question must be provided at a distance, by electronic means and at the request of the recipient of the service.

<sup>478</sup> See recital 48 of directive (EU) 2016/1148.

<sup>479</sup> See recital 49 of directive (EU) 2016/1148.

<sup>480</sup> European Commission, ‘Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 Laying down Rules for Application of Directive (EU) 2016/1148 of the European Parliament and of the Council as Regards Further Specification of the Elements to Be Taken into Account by Digital Service Providers for Managing the Risks Posed to the Security of Network and Information Systems and of the Parameters for Determining Whether an Incident Has a Substantial Impact’, 30 January 2018, C/2018/0471, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R0151>.

<sup>481</sup> See article 16(7) of directive (EU) 2016/1148.

digital service provider does not meet the requirements laid down in Article 16"<sup>482</sup>.

The effectiveness of supervision is further hampered by the difficulty of identifying the main establishment of each digital service provider. Although it is not necessary to identify them in advance, the capillarity with which digital services are provided means that it cannot be taken for granted that regulatory authorities will know which providers of essential services are present on their territory.

Indeed, some commentators have questioned whether there is any justification for favouring digital service providers. It should be recalled that ENISA itself had argued against over-burdening these actors with red tape, as this could limit the EU's ability to respond quickly and efficiently to cyber incidents<sup>483</sup>.

In general, it can be said that this tendency to avoid overburdening these issues is reflected in a number of provisions in the Directive. Even where it recognises perfectly legitimate interests in the protection of sensitive national interests, a kind of paternalism emerges, sometimes expressed as a proposal for alternatives. For example, while recognising the interest in better protection of cloud infrastructures, it calls for this need to be addressed through contractual obligations rather than through the imposition of further obligations at national level<sup>484</sup>.

### III.2.2 The NIS reform

Although the European Union had high hopes for the NIS system, less than a year before the implementation deadline of 9 May 2018, the Commission began to express its doubts. An ongoing review emphasised that implementation efforts would necessarily have to go beyond the minimum requirements of the Directive in order to achieve a truly holistic approach. Cybersecurity is a relatively new and rapidly evolving area, so ambitious decisions had to be taken that would allow security measures to become integrated and structural. Member States needed to focus on improving their own responsiveness, but the diversity of approaches and the often high degree of decentralisation at national level threatened to frustrate efforts. The system of contract points deserved to be strengthened, while at the same time extending its scope to other key sectors, in particular public administration, had already been recommended. Despite the recommendations for effective implementation, the overall effectiveness of the intervention needs to be reviewed.

At the same time, the positive results should not be downplayed. It is certainly important to recognise how the Directive has laid the foundations for robust cybersecurity capabilities at national level, both through the imposition of national strategies and the creation of national authorities. The establishment of competent authorities has simplified the management of relations both within and between Member States. Moreover, on the basis of this common organisation, two new supporting bodies had been created at European level, the Cooperation Group and the Network of CSIRTs, which had contributed to the creation and dissemination of common practices. In this way, the level of harmonisation had been improved and a solid basis for discussing issues related to cybersecurity regulation had been established. For example, the cooperation group had made an important contribution to 5G

---

<sup>482</sup> See article 17(1) of directive (EU) 2016/1148.

<sup>483</sup> Dimitra Markopoulou, Vagelis Papakonstantinou, and Paul De Hert, 'The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation', *Comput. Law Secur. Rev.* 35 (2019): 6, <https://doi.org/10.1016/J.CLSR.2019.06.007>.

<sup>484</sup> See recitals 54 and 56 of directive (EU) 2016/1148.

security during the development of the so-called 5G toolbox. As far as new European bodies are concerned, the activities of the Cyber Crises Liaison Organisation Network ("CyCLONe") should also not be overlooked, although it initially had only an informal role as part of the broader design of a blueprint for rapid emergency response.

"More advanced policy responses in the field of cybersecurity have become a matter of urgency, as the number of cyber-attacks continues to rise, with increasingly sophisticated attacks coming from a wide range of sources inside and outside the EU"<sup>485</sup>.

What were initially incidents caused by natural disasters or criminal organisations have become full-blown acts of cyber warfare perpetrated by state actors.

Cybersecurity has become one of the European Union's cross-cutting priorities under the new Digital Single Market strategies. In 2016, the European Parliament called for a significant improvement in cyber resilience, in parallel with measures to support the digitisation of the market, through a stronger role for ENISA<sup>486</sup> and national CERTs<sup>487</sup>, the creation of which should be accelerated.

In general, discourses on resilience have been accompanied by the entrenchment of the principle of security by design, which aims to reverse the traditional logic of ex-post intervention when vulnerabilities are identified<sup>488</sup>. As early as 2019, the Commission was invited to assess the need to further extend the scope of the NIS Directive to other critical areas<sup>489</sup>. This request will be taken into account in the development of the "Shaping Europe's Digital Future" projects.

"European technological sovereignty starts from ensuring the integrity and resilience of our data infrastructure, networks and communications. It requires creating the right conditions for Europe to develop and deploy its own key capacities, thereby reducing our dependency on other parts of the globe for the most crucial technologies"<sup>490</sup>.

This is why, among other initiatives, a new cyber security strategy has been advocated<sup>491</sup>,

---

<sup>485</sup> European Commission, 'COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Accompanying the Document Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity across the Union, Repealing Directive (EU) 2016/1148', 16 December 2020, 11, SWD(2020) 345 final, [https://eur-lex.europa.eu/resource.html?uri=cellar:d51e4bbb-3fa8-11eb-b27b-01aa75ed71a1.0001.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:d51e4bbb-3fa8-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF).

<sup>486</sup> European Parliament, 'European Parliament Resolution of 19 January 2016 on Towards a Digital Single Market Act', 19 January 2016, 21, 2015/2147(INI), [https://www.europarl.europa.eu/doceo/document/TA-8-2016-0009\\_EN.pdf](https://www.europarl.europa.eu/doceo/document/TA-8-2016-0009_EN.pdf).

<sup>487</sup> European Parliament, 'European Parliament Resolution of 3 October 2017 on the Fight against Cybercrime (2017/2068(INI))', 11.

<sup>488</sup> European Parliament, 11.

<sup>489</sup> European Parliament, 'European Parliament Resolution of 12 March 2019 on Security Threats Connected with the Rising Chinese Technological Presence in the EU and Possible Action on the EU Level to Reduce Them (2019/2575(RSP))', 12 March 2019, 4, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019IP0156>.

<sup>490</sup> European Commission, 'COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Shaping Europe's Digital Future', 19 February 2020, 2, COM/2020/67 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0067&qid=1641573209491>.

<sup>491</sup> European Commission, 7.



one of the main objectives of which is precisely the reform of the NIS system<sup>492</sup>.

The same order of priorities was shared by the Council of the European Union<sup>493</sup>, which welcomed the Commission's positions and called for an acceleration of the secure development of the latest generation of network infrastructures<sup>494</sup> and a review of other sectoral legislation, in particular the preparation of a measure introducing minimum security requirements for network-connected devices<sup>495</sup>.

On the basis of this statement of intent, the results of the first Directive have been carefully examined in order to design future reform measures, as required by Article 23 of the NIS Directive itself. The evaluation carried out by the Commission and annexed to the new Directive was based on questionnaires sent to various stakeholders. The responses had revealed a number of major shortcomings, which could be grouped into a number of themes<sup>496</sup>.

Firstly, the low level of resilience achieved by businesses and, more generally, by all those covered by the legislation, which was only at an intermediate level<sup>497</sup>. Although many companies had made remarkable progress in just a few years, the EU's overall level of resilience remained low, especially when compared to other more advanced countries. This has been exacerbated by the rapidly changing digital landscape. The main reason for these shortcomings was the limited number of sectors covered by the legislation, which resulted in fewer operators being subject to minimum security obligations. As a result, many countries had autonomously decided to extend the scope of the regulation. The problem of defining an effective scope is crucial given the high degree of interconnectedness between actors, which gives rise to externalities that are difficult to control. Many companies may have no interest in improving their security posture if they know that the cost of implementing security measures will be borne by others. As a result, those who are not regulated and who rely on parties who are obliged to invest in security instead, have no incentive to invest in the same way and benefit from the best protection at no cost.

The second problem, partly related to the first, was the existence of different levels of resilience between different Member States and sectors. In other words, not only is it crucial to be able to define which sectors are covered by the legislation, but above all which operators in those sectors are actually required to comply with the obligations. It is therefore necessary to take into account the inconsistencies in the procedure for identifying operators of essential services within the same sector, which have resulted in the same category of entities being covered or not being covered by the Regulation depending on the Member

---

<sup>492</sup> See paragraph II.3.4 for further details on the last strategy.

<sup>493</sup> Council of the European Union, 'Council Conclusions on Shaping Europe's Digital Future', 16 June 2020, 6, 2020/C 202 I/01, [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020XG0616\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020XG0616(01)).

<sup>494</sup> Council of the European Union, 'Special Meeting of the European Council (1 and 2 October 2020) – Conclusions', 2 October 2020, 4, <https://data.consilium.europa.eu/doc/document/ST-13-2020-INIT/en/pdf>.

<sup>495</sup> Council of the European Union, 'Council Conclusions on the Cybersecurity of Connected Devices - Council Conclusions Approved by Written Procedure', 2 December 2020, 6, <https://data.consilium.europa.eu/doc/document/ST-13629-2020-INIT/en/pdf>.

<sup>496</sup> The following considerations are taken from European Commission, 'COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Accompanying the Document Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity across the Union, Repealing Directive (EU) 2016/1148', 15–29.

<sup>497</sup> European Commission, 17.

State. Despite the fact that the competent authorities throughout the Union had identified thousands of public or private entities, there were still major differences in the implementation of the identification rules, leading to differences in treatment, sometimes quite marked. This has led not only to heterogeneous levels of cybersecurity, but also to restrictions on the internal market, especially for those entities that are mainly active across borders and have to bear the bureaucratic burden of different requirements.

From a certain point of view, this was a waste of resources invested in compliance rather than in a real increase in safety. Not to mention the fact that the level of control by the authorities had not reached a satisfactory level in any case, so that the measures had to be complied with. Even if part of the problem can be attributed to a design choice of the Directive, the different methodologies adopted by Member States have certainly exacerbated the problem.

The existence of an identification process could be effective in ensuring the resilience of critical infrastructure against non-digital threats, but the resulting excessive fragmentation made it impossible to guarantee an adequate level of cyber protection due to the undeniable interconnections between different actors. Of course, these remarks only applied to operators of essential services and not to digital service providers, for whom no prior identification was required. For the latter, the complication was not so much in identifying them as in identifying the jurisdiction to which they were subject. On the one hand, digital service providers in several EU countries must be subject to the jurisdiction of the country in which they have their main establishment. On the other hand, in the case of providers established outside the EU, the Directive requires them to appoint a representative in one of the Member States in order to be subject to the jurisdiction of that Member State. The problem is that suppliers are not obliged to inform the competent national authority of the appointment of a representative. In addition, the national authorities themselves do not have sufficient powers to independently verify which suppliers, both EU and non-EU, are actually subject to their jurisdiction.

In addition to the difficulties in identifying those subjects to the regulations, there was also complexity in the measures they had to implement because of the wide discretion left to Member States. The safety measures varied considerably, as did the thresholds for assessing compliance with the criteria for submitting an incident report to the competent authority. Notification procedures also varied considerably.

The national authorities themselves, in the absence of precise standards to which they could adhere, took very different measures in exercising their control, given the same number of infringements found. Sanctions varied considerably in both type and level, but most authorities were reluctant to apply them. This largely reflected the different levels of cyber capabilities developed by Member States, with different political priorities and budgets allocated to security.

Finally, the third problem that emerged was the low level of situational awareness and the consequent limited ability to respond. Indeed, Member States did not share information on the state of cyber security among themselves, and did not even have comprehensive reports, as there were no structured channels for cooperation with the private sector. The European bodies themselves had failed in their aim to promote more efficient exchanges, which remained limited and rather sporadic. A systematic approach was far from being established. Neither the cooperation group, nor the CSIRT network, nor the Commission were able to successfully analyse attacks at a European level in order to define the most vulnerable sectors

in a comparative manner across countries. The main reason for this inefficiency was the generality of the Directive's provisions on cooperation, which, due to their abstract nature, had led to cooperation being interpreted simply as voluntary.

As a result, very few countries had used the cross-border consultation procedure. However, even where it had been used, it had not produced any real results due to the lack of more detailed information on how it would work. In particular, the establishment of a platform to facilitate the exchange of sensitive information would have been useful. The bodies at European level did not have complete information on safety, because the whole system was based on the reporting of incidents, leaving out other information, however important, such as the level of qualification and training of personnel. All this prevented the real implementation of a crisis management mechanism, since the legislation only dealt with the accident notification phase<sup>498</sup>.

All the shortcomings identified were rooted in the regulatory framework and would have been difficult to remedy without action. On the contrary, a worsening of the situation with an increase in accidents could have been expected, which would have led to an increase in safety-related costs. Many private actors might have been able to increase their investments, but the overall performance would still have been uneven, in particular because of the significant externalities.

For all these reasons, the European legislator had decided, following its impact assessment, to proceed with the amendment of the NIS Directive and its replacement. The final text of the so-called NIS2 was adopted in December 2022 and must be implemented by 17 October 2024, in time for the repeal of the previous directive.

The fact that the Directive retains its basis of legitimacy in Article 114 TFEU demonstrates the usual strong link of the intervention to the internal market. If “incidents can impede the pursuit of economic activities in the internal market [...]” “cybersecurity is a key enabler for many critical sectors to successfully embrace the digital transformation and to fully grasp the economic, social and sustainable benefits of digitalisation”<sup>499</sup>.

As has just been shown, the excessive discretion left to the Member States has limited the positive effects of harmonisation and has had a negative impact on the logic of the market, with many different requirements to be implemented by different operators. In addition, the fragmentation of the measures has created an inherent uncertainty that could be exploited by attackers<sup>500</sup>.

---

<sup>498</sup> The cybersecurity crisis management cycle generally consists of four phases: preparation, response, recovery and lessons learned. In the preparation phase, organisations proactively assess their vulnerabilities, develop incident response plans, and implement security measures. During the response phase, they detect and respond to a cyber incident, contain the breach, mitigate the damage and investigate the cause. The recovery phase focuses on restoring normal operations, repairing affected systems and implementing stronger security measures. Finally, the lessons learned phase involves conducting post-mortem evaluations to identify weaknesses, update plans and controls, and improve future incident response capabilities. See G r me Billois, ‘Cybersecurity Incident and Crisis Management’, in *The Cyber Risk Handbook* (John Wiley & Sons, Ltd, 2017), 171–84, <https://doi.org/10.1002/9781119309741.ch12>.

<sup>499</sup> European Parliament and Council of the European Union, ‘Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive)’, 333 OJ L   (2022), para. 3, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555>.

<sup>500</sup> European Parliament and Council of the European Union, para. 5.

This explains the special attention given to the new scope. First, there are two major additions to the scope. On the one hand, rules and obligations for the exchange of cybersecurity information, and on the other hand, specific obligations to carry out monitoring and enforcement activities. These were two important omissions that were one of the main causes of the inefficiency of the NIS system, precisely because it was still based on a mistaken belief in the efficiency of voluntary cooperation and implementation.

The scope of application is modelled by the introduction of objective and unambiguous criteria for the identification of subjects, in particular the size of the enterprise. Thus, within the sectors defined in the first two annexes<sup>501</sup>, all entities that are at least medium-sized fall within the scope of the Regulation. On the basis of this initial selection, further additions will be made, regardless of the size of the entity<sup>502</sup>, while always retaining the possibility of certain exclusions justified by the performance of activities related to national security or essential State functions.

Although not new, there is also an effort to coordinate with other European legislation, through references to the DORA regulation on resilience in financial activities, the GDPR and the e-privacy directive, and the new directive on critical infrastructure. This time, however, there is more attention, which is also reflected in the increased space devoted to the issue in the recitals. Furthermore, Article 4 finally introduces objective criteria to define the relationship with other sectoral legislation. As in the first directive, the more specific legislation must take precedence if it introduces at least equivalent obligations. However, this equivalence is specified in terms of minimum safety measures and incident reporting. In short, a sectoral regulation can only prevail if it requires equivalent security measures in its effects and its incident reporting obligations allow immediate access to notifications to the CSIRT and other NIS authorities.

As regards more specifically the way in which the scope is defined, the previous distinction between essential service operators and digital service providers is no longer relevant in today's society. The system is still based on a dual regime, but between essential and important entities, listed in Annexes I and II respectively.

As shown in Figure 16, Article 3 defines the distinction in two concentric groups, which contributes to a considerable simplification. All entities identified on the basis of Article 2, i.e. on the basis of the sectors of the Annexes, are covered by the Regulation, the obligations of which mainly concern the core entities. The latter represent the core group of entities identified on the basis of size and other criteria related to the type of activity carried out. Note that, unlike the first Directive, there is no clear distinction between the Annexes. Although the size criterion is applied only to entities in the first Annex, the wording of Article 2 does not prevent entities in the sectors of Annex II from being identified as core entities. In addition, concentric circles are created because the identification of important entities is

---

<sup>501</sup> The sectors are in line with those of the critical infrastructure legislation already examined in the paragraph on critical infrastructure. See in particular Figure 11. In addition, postal and courier services, waste management, and others are defined as "other critical sectors".

<sup>502</sup> See article 2 of directive (EU) 2022/2555. Consider providers of public electronic communications networks or of publicly available electronic communications services, trust service providers, and top-level domain name registries and domain name system service providers. However, the most relevant additions are certainly those relating to critical infrastructures and public administration, possibly also at local level, if the Member State so decides. Furthermore, the focus on research institutes, which could also be included, is not secondary.

negative with respect to essential entities. In other words, all entities that are not identified as essential entities are automatically to be considered as important entities.

However, if this were the end of the logic behind the distinction, Figure 16 would be wrong. The outermost level exists because not all the entities referred to in the annexes necessarily fall within the scope. European legislation cannot be applied in conflict with national security or the performance of essential state functions. Consequently, the Directive does not apply to those public administrations which represent these interests or which are involved in the investigation or prosecution of criminal offences. Other exceptions can be identified.

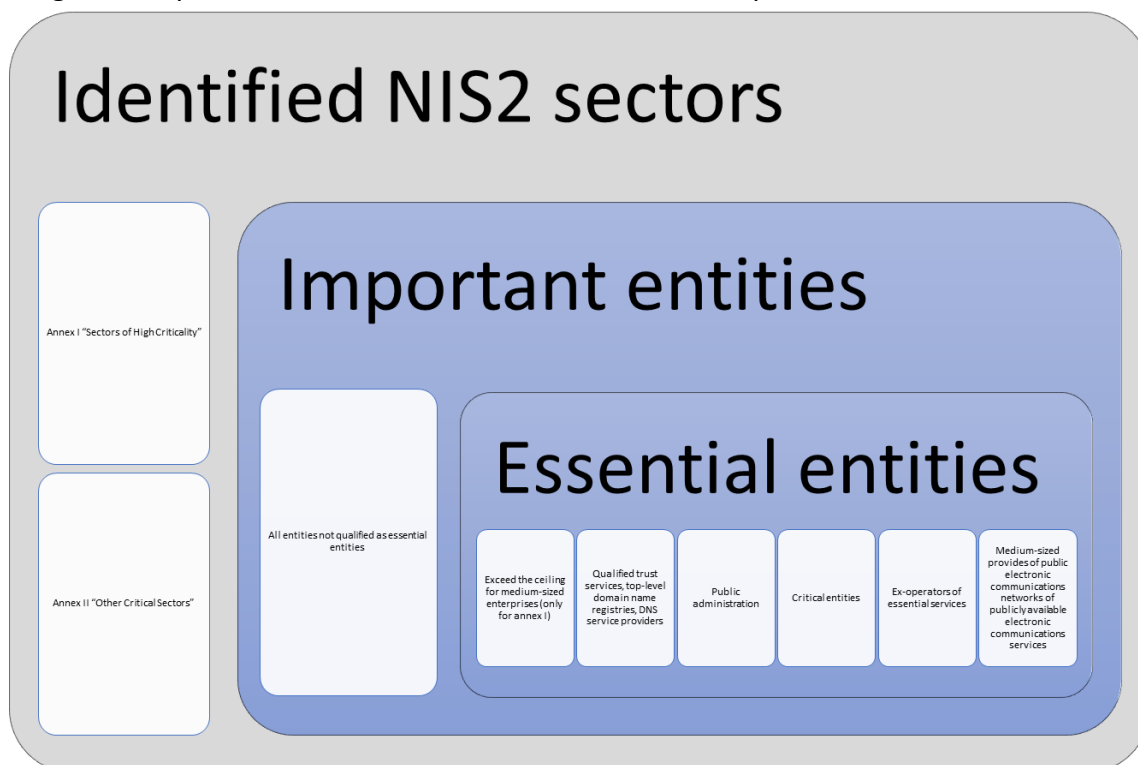


Figure 16 - Scope of NIS2 directive

In terms of national organisation, one of the key obligations is the adoption of a national cyber security strategy, which is detailed. Among the most important additions are the supply chain and information sharing issues, which are highlighted throughout the new Directive.

In addition to the obligation to designate competent authorities, one of which will be a contact point, there is also the introduction of competent authorities for major cyber incidents and crisis management. These are referred to in the technical jargon as cyber crisis management authorities, one of which must play the role of coordinator. This means that the national cyber security strategy must be accompanied by a plan for the management of major cyber incidents and crises, clearly identifying the authorities' capabilities, the resources at their disposal and the procedures to be followed. This important innovation at national level corresponds at European level to the formal institutionalisation of the European Cyber Crisis Liaison Organisation Network (EU-CyCLONE), which is a fundamental building block within the European crisis response system<sup>503</sup>.

<sup>503</sup> EU-Cyclone is composed of representatives of the national authorities for cybercrisis prevention and the Commission, which plays an observer role unless a major incident could have a significant impact on the areas covered by the Directive. ENISA provides the secretariat. The main objective is to enhance the preparedness of

The need to maximise the synergies between the various players and to strengthen coordination was recognised more than a decade ago in the conclusions of the Council of the European Union, which encouraged the Member States to participate in the development of a European system for cooperation in the event of accidents<sup>504</sup>. However, the first concrete results are relatively recent, as they followed the Commission's idea of consolidating a crisis response approach by exploiting existing elements in the European ecosystem. Although the NIS system did not take this aspect into account, it was suggested that the necessary logic be grafted onto it in order to make the most of the existing system of cooperation<sup>505</sup>. Since “knowledge and expertise on cybersecurity [was] available at the EU level, but in a dispersed and unstructured way”<sup>506</sup>, the idea was to frame it in a coherent way.

The result of this effort was a blueprint, annexed to a Commission Communication, which attempted to bring all existing cyber actors and procedures into an organised system, creating different levels of response<sup>507</sup>.

A few years later, this system would be further complemented by the creation of EU-CyCLONe, which would establish itself as a link between the political<sup>508</sup> and technical levels in crisis management, laying the foundations for a stable network of cooperation between Member State authorities<sup>509</sup>. Its first annual test took place in 2020, during the second edition of Blue OLEx<sup>510</sup>, a series of cybersecurity tests and exercises launched in 2019<sup>511</sup>. However, new impetus for the whole system came in particular from the COVID-19 wave, during which discussions on the creation of a Joint Cyber Unit “to respond together and exchange

---

Member States through information exchange for the benefit of collective situational awareness.

<sup>504</sup> European Commission, ‘Commission Recommendation (EU) 2017/1584 of 13 September 2017 on Coordinated Response to Large-Scale Cybersecurity Incidents and Crises’, 9.

<sup>505</sup> European Commission, ‘COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - Strengthening Europe’s Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry’, 4.

<sup>506</sup> European Commission, 4.

<sup>507</sup> The response to cybersecurity incidents could take many forms, from operational decisions on security measures to political decisions involving a diplomatic response. In describing its architecture, the blueprint itself had three levels, depending on the actors involved. One political, one operational and one technical. For a detailed discussion of its components, see European Commission, ‘Commission Recommendation (EU) 2017/1584 of 13 September 2017 on Coordinated Response to Large-Scale Cybersecurity Incidents and Crises’, 13.

<sup>508</sup> The organisation of crisis management at political level is based on the EU's Integrated Political Crisis Response (IPCR) arrangements, which implement the European Solidarity Clause. The IPCR has been adapted by a recent implementing decision of the Council of the European Union. See Council of the European Union, ‘Council Implementing Decision (EU) 2018/1993 of 11 December 2018 on the EU Integrated Political Crisis Response Arrangements’, 320 OJ L § (2018), [http://data.europa.eu/eli/dec\\_impl/2018/1993/oj/eng](http://data.europa.eu/eli/dec_impl/2018/1993/oj/eng).

<sup>509</sup> ‘EU CyCLONe’, Topic, ENISA, accessed 31 August 2023, <https://www.enisa.europa.eu/topics/incident-response/cyclone>. See recital 71 of the directive (EU) 2022/2555.

<sup>510</sup> To be precise, it was a table-top exercise. A table-top exercise is a simulated scenario-based training activity conducted in a tabletop setting, typically involving key stakeholders and decision-makers. It aims to assess and enhance preparedness, response, and coordination capabilities in the event of a real-world incident or crisis. Participants discuss and analyse the scenario, identify potential challenges, and collectively develop strategies and actions to mitigate and address them. The exercise is conducted in a controlled environment without active deployment of resources.

<sup>511</sup> The last edition was held in Vilnius on 7 November 2022.

information on a 'need to share' [...] basis" had flourished<sup>512</sup>. This would have made up for the lack of a European platform for information exchange and thus improved the conditions for solidarity, without necessarily creating a new body at European level.

In general, there is a broadening of attention to other aspects of cybersecurity, a sign of increased awareness. Another important example, still at national level, is the requirement to establish a mechanism to support the disclosure of vulnerabilities found in ICT products or services. This is the standardisation of critical aspects for a digital society where the resilience of its essential components is tested every day by new attacks. Each of these tends to exploit known and unknown vulnerabilities, which is why the constant enrichment of knowledge on the subject is essential to prevent the success of any attacker. At the same time, it is a delicate process.

Anyone who discovers a new vulnerability and chooses to report it must be supported so that the disclosure of the discovery benefits society but does not harm potentially affected entities, giving them time to implement appropriate countermeasures. This is usually done by negotiating a deadline after which the vulnerability is published. This publication will take place in a European database created and maintained by ENISA, which will be the unifying aspect of the vulnerability disclosure system at European level<sup>513</sup>.

The final observation on the organisation at national level concerns the cooperation between the different authorities, which has reached a high level of maturity. One can clearly see the effort to create a connecting system in order to ensure an alignment of cyber security knowledge. For this reason, the NIS should no longer be seen as a separate system, but as a connecting regulation between actors and bodies that emerge in different contexts and with different competences. In particular, the initially implicit overlap with the data breach procedures contained in the GDPR will be made explicit and regulated. Whenever a cyber incident involves personal data, the NIS authorities must immediately inform the DPA<sup>514</sup>, also to avoid unnecessary duplication of sanctions.

At the European level, there is also a clear maturation of cyber awareness. Whereas previously ENISA's reports were mainly based on information on incidents, the areas of interest are broadening to include other inherent aspects such as the level of cyber capabilities, good security practices and training. Nor is it secondary that all future reports will be available in an automated format.

As well as increasing the amount of information available, it will also increase accountability through the introduction of a voluntary peer review mechanism, the aspects of which will be defined by the cooperation group. This could become a tool for the growth

---

<sup>512</sup> European Commission, 'COMMISSION RECOMMENDATION on Building a Joint Cyber Unit', 23 June 2021, 1, C(2021) 4520 final, <https://ec.europa.eu/newsroom/dae/redirection/document/77514>.

<sup>513</sup> Vulnerability management has long been neglected on the old continent, unlike the United States, where all the most common databases used by insiders are maintained. Note that not all of these are necessarily maintained by public bodies. For example, the most famous and widely used is certainly the Common Vulnerability Exposure (CVE) database maintained by MITRE, a historic American cybersecurity company. The database can be found on their website 'Home | CVE', accessed 1 September 2023, <https://www.cve.org/>. Another well-known vulnerability database is that of the US NIST. Regardless of the database consulted, each vulnerability is searchable by a unique and progressive code CVE-YYYY-NNN. This is possible because each disclosure request is blocked by a so-called CVE Numbering Authority (CNA), which can be an ICT product or service provider, a CERT or a bug bounty organisation. More details on how this works can be found at 'NVD - Vulnerability Status', accessed 1 September 2023, <https://nvd.nist.gov/vuln/vulnerability-status>.

<sup>514</sup> See articles 13 and 35 of the directive (EU) 2022/2555.

and standardisation of cyber capabilities among different countries through objective peer review. The idea is not to point out the shortcomings of a requesting Member State, but to provide technical assistance to improve its own security practices<sup>515</sup>.

The most interesting part of the regulation, however, is the part relating to governance. The two basic obligations to take appropriate security measures and to report incidents are maintained.

The first aspect to note is that, unlike the situation between essential service operators and digital service providers, both obligations do not apply differently depending on whether one is an essential or an important entity. In general, however, a risk-based approach remains, understood as risk from any type of threat. The rationale is to implement those measures which, taking into account the state of the art, are most effective in improving the risk situation at the same cost<sup>516</sup>. Categories of measures<sup>517</sup> are listed to assist in identification, including those related to supply chain protection. The issue of supplier relationships is strongly emphasised, as the NIS Co-operation Group will carry out a coordinated risk assessment of certain critical supply chains identified by the European Commission<sup>518</sup>, in order to assist stakeholders in selecting the most appropriate protection measures. In such a case, it is suggested that the parties also implement security through contractual agreements<sup>519</sup>.

Although the approach is at least apparently similar, the unified Article 21 does not reflect the unifying character of the NIS Directive, which is intended to become the single reference point for both the implementation of security measures and the notification requirements. Consequently, since providers of trust services, public electronic communications networks or publicly available electronic communications services are now included in the scope of the new NIS, the corresponding provisions in the respective sectoral legislation will have to be deleted<sup>520</sup>.

---

<sup>515</sup> See article 19 of the directive (EU) 2022/2555.

<sup>516</sup> The rationale is based on a well-established international standard which is mentioned in the recitals referring to the ISO 27000 series. In order to prevent safety from becoming an unnecessary bureaucratic burden, measures should always be proportionate to the likelihood of accidents occurring and the severity of their effects. In any case, the application of international standards is considered as an alternative to the existence of certification schemes under the Cybersecurity Act.

<sup>517</sup> The technical and methodological measures to be adopted, together with the appropriate requirements, may be laid down in specific implementing acts of the Commission. In particular, for service providers who, by the nature of their business, are established in several countries of the Union, this identification must be carried out by 17 October 2024.

<sup>518</sup> See article 22 of the directive (EU) 2022/2555. At the time of writing, ENISA has published a summary report of the main cybersecurity best practices adopted in the supply chain to support the future work of the Cooperation Group. See ENISA, 'Good Practices for Supply Chain Cybersecurity', June 2023, <https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity/@download/fullReport>. According to the analysis in the summary, future analysis should be similar to that already undertaken for the Next Generation Telecommunications sector. See European Commission, 'Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G Networks', 26 March 2019, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019H0534>.

<sup>519</sup> See recital 85 of the directive (EU) 2022/2555.

<sup>520</sup> This repeal is provided for in Articles 42 and 43 and will take effect on 18 October 2024. In any case, the Directive seeks to ensure as much continuity as possible with the previous system, on the one hand by taking into account all the material prepared at national and European level for the correct application of the sectoral rules. It also suggests that Member States designate sectoral authorities as NIS authorities to ensure continuity.



The second relevant obligation is the obligation to notify incidents that have a significant impact on services, for which the definition criteria have been unified and simplified, and those incidents that could adversely affect the provision of services. This second category of incidents is a useful addition in order not to exclude useful information from the obligation to notify, even if it does not concern an incident of such seriousness as to fall under the first category. In addition, precise time limits have been set for the different phases of the incident notification process, which, following the practice established in the first Directive, should be understood as a dynamic exchange of information in several phases between the entity concerned and the CSIRT.

Broadly speaking, the key moments of this exchange are reminiscent of those already highlighted for the first NIS Directive, with the addition of the possible interim report, depending on the needs of the CSIRT. Another relevant difference concerns the final report, which is divided into two distinct moments. Looking briefly at the stages shown in Figure 17, the initial aim remains to inform the CSIRT of the existence of the incident, and only at the time of the actual notification should an initial impact assessment be made, with any available indicators of impairment. Only after a reasonable period of time should more structured information be provided in a report, which should include a detailed description, including the mitigation measures taken. If the incident lasts longer than one month after notification, a post-recovery report must also be prepared. The intention of the European legislator is to prevent an excessive amount of time passing without more detailed information to the CSIRT.

Certainly, more information will be specified by the Commission, which will have to adopt its own implementing act by 17 October 2024 in order to specify the concept of a major accident for certain categories of establishments that are particularly widespread in the Union. However, it is also left to the Commission to further specify the type of information, the format and the notification procedure.

---

There should be coordination between these authorities and the NIS authorities. See recitals 94 and 95 of Directive (EU) 2022/2555.

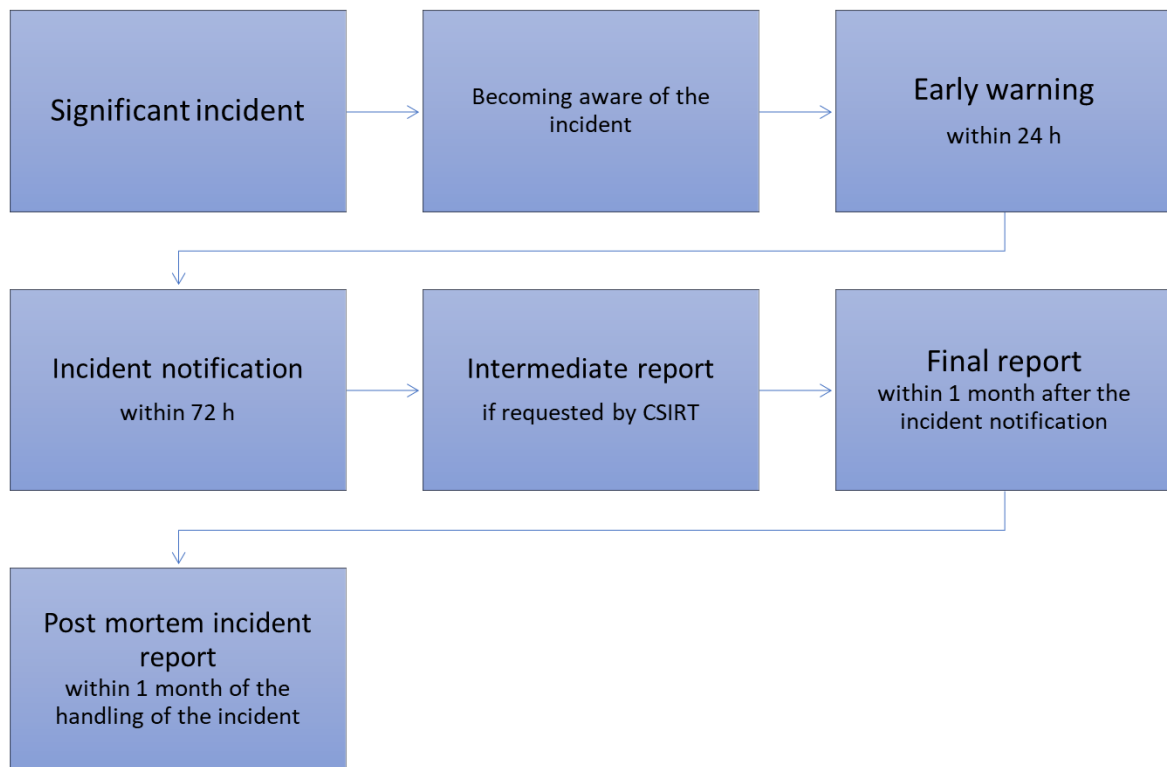


Figure 17 - Incident notification procedure according to NIS2

Finally, a final peculiarity concerning the reporting of incidents can be found in the provisions on voluntary reporting<sup>521</sup>, which introduces the concept of “near misses”<sup>522</sup>. In fact, voluntary notification does not only concern entities outside the scope of the Regulation, but also essential and important entities, which have the possibility to notify even those events that could potentially affect their data or services. The effectiveness of this option will work in synergy with any voluntary agreements for the exchange of relevant cybersecurity information. Such agreements may involve both external and internal actors<sup>523</sup>.

In view of the many problems caused by the lack of clarity as to the jurisdiction applicable to different entities, the new Directive devotes much more space to defining their proper location. The main criterion is that of establishment, according to which an entity is simply subject to the jurisdiction of the country in which it is established. However, this is followed by a number of exceptions, shown in Figure 18, concerning entities whose activities are characterised by a predominant cross-border dimension.

<sup>521</sup> See article 30 of the directive (EU) 2022/2555.

<sup>522</sup> The definition in Article 6(5) is as follows “‘near miss’ means an event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but that was successfully prevented from materialising or that did not materialise”.

<sup>523</sup> See article 29 of the directive (EU) 2022/2555.

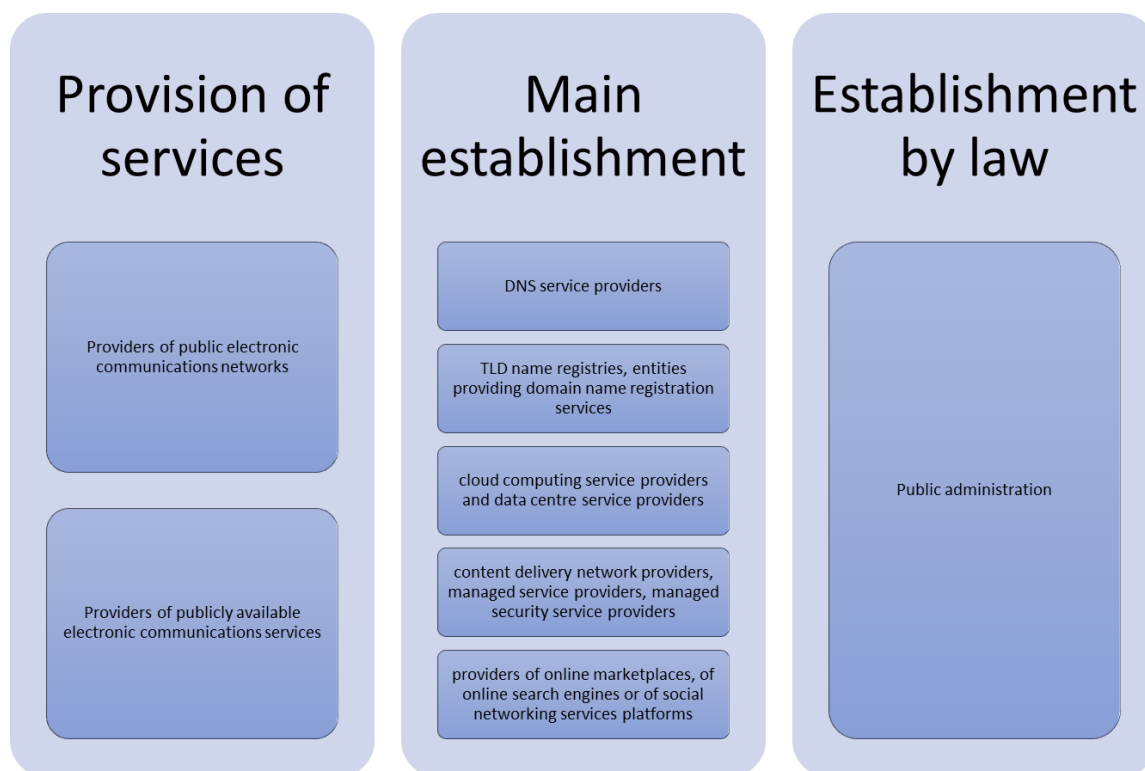


Figure 18 - Summary of the NIS2

In particular, for those entities to which the principal establishment criterion applies, an alternative set of objective parameters is provided for their correct identification. However, the most important innovation is undoubtedly the creation of a register of entities at ENISA, in which information will be collected on precisely those entities that are subject to the principal establishment criterion, to avoid any doubt as to the application of jurisdiction. In order to populate the register, the competent authorities of the Member States will have to carry out a first phase of information gathering by 17 January 2025 and then forward the results to ENISA through its contact point<sup>524</sup>.

In general, one of the biggest changes brought about by NIS2 is the focus on the proper maintenance of registries, including those that already exist. One example is the registries containing the registration data of domain names, the so-called WHOIS data. The accuracy and publicity of such data is essential to prevent DNS abuse, so specific ex-ante and ex-post controls must be applied to registration, and at least the data for legal entities should be made public<sup>525</sup>.

A final issue to which the European legislator has devoted space is that of supervision and control measures by the competent authorities of the Member States. Whereas the first Directive only required the general allocation of adequate powers and resources, the new text not only requires effective, proportionate and dissuasive measures, but also provides a list of minimum supervisory powers and minimum control powers<sup>526</sup>.

Although this list is not exhaustive, it certainly has the merit of promoting the harmonisation of powers at Union level, while at the same time attempting to strike a balance

<sup>524</sup> See article 27 of the directive (EU) 2022/2555.

<sup>525</sup> See recitals from 109 to 112 of the directive (EU) 2022/2555.

<sup>526</sup> See article 32(2)(4) of the directive (EU) 2022/2555.

between the imposition of sanctions and the exercise of the right of defence in the appropriate fora, considering the seriousness of the infringement, its duration and the damage caused. Measures must certainly be proportionate to the risk posed by the infringement, but the possibility of an adversarial procedure must always be guaranteed. In this regard, a procedure is also outlined that should ideally precede the imposition of sanctions. The competent authority should always communicate its preliminary findings to the undertakings concerned, in order to allow them a reasonable time to comment.

Despite this significant evolution, which has led to the explicit reference to fundamental rights in the operational part of the regulatory text, the idea of a dual track between essential and important entities remains. For the latter, intervention measures can only be ex post, as is the case between operators of essential services and providers of digital services.

Finally, with regard to sanctions, on the one hand, minimum and maximum thresholds for administrative sanctions are introduced in order to overcome the extreme fragmentation caused by the total absence of guidelines. On the other hand, criminal sanctions are explicitly mentioned, the introduction of which will therefore be obligatory for all Member States, which will have to notify the Commission of the implementing provisions.

In the absence of further action by the European institutions, transposition at national level will have to take place by 17 October 2024, after which the old Directive will be repealed<sup>527</sup>. The date for the first review of the effects of NIS2 is set for 17 October 2027, three years after the first application of the effects. Although it is too early to make a final judgement, the measures seem to take into account the shortcomings of the previous system and bode well for its future effectiveness.

However, there is no shortage of criticism of the fact that the European legislator has once again chosen the instrument of a directive. It is true that the great diversity of national scenarios led to this choice, but it exposes the EU to the same problems of uncertainty that characterised the previous system. What may be seen as adaptability on the one hand may be a lack of interoperability on the other<sup>528</sup>.

The functioning of the new regulatory regime will have to await transposition into national law before it can be properly assessed. There are very different situations, ranging from countries that have already set up their own more or less compliant national systems, to others for whom the new NIS will be an opportunity to completely restructure their internal system<sup>529</sup>.

---

<sup>527</sup> Annex III contains a transposition table to transfer all references to the old Directive to the updated provisions.

<sup>528</sup> Buffa, 'La Direttiva NIS II Cybersecurity in Europa', 62–63.

<sup>529</sup> Sandra Schmitz-Berndt and Pier Giorgio Chiara, 'One Step Ahead: Mapping the Italian and German Cybersecurity Laws against the Proposal for a NIS2 Directive', *International Cybersecurity Law Review* 3, no. 2 (1 December 2022): 289–311, <https://doi.org/10.1365/s43439-022-00058-7>.

## IV The Italian Cybersecurity Perimeter

As amply demonstrated in the chapter III on the sources of EU law, the attempt to circumscribe the acts of interest in terms of cybersecurity policy leads to the definition of a rather heterogeneous set. Although the analysis can be carried out in a systematic way, the same result is reflected in the national legal horizon, which is strongly influenced by EU policies.

To avoid redundancy, the analysis will focus on the most representative aspects that differ somewhat from the EU framework. Most of the areas shown in Figure 42 have resulted in transposition legislation. Consider the issue of digital identity and trust services, which has been accompanied by a reform of public administration, which could have benefited from the new possibilities offered by digitalisation to improve the accessibility and quality of its services to citizens<sup>530</sup>. The same can be said, even more so, for all those areas closely related to cybersecurity in the strict sense, such as critical infrastructure, NIS, certification, not to mention the infinite number of measures to protect personal data. If privacy is constantly expanding with the introduction of new technologies<sup>531</sup>, the reciprocal links with cybersecurity are now another distinguishing feature<sup>532</sup>.

Each of these topics undoubtedly warrants a separate and more detailed examination. However, within the context of this research, it is essential to maintain a focus on the National Cybersecurity Perimeter, which aligns with the broader goals of the ERACLITO project.

Given the need to refine the scope, the selection criterion for topics is based on national developments. As expected, the focus will be on those developments in the country's cybersecurity that do not depend on or implement a primary act of the European Union.

The objective is to define the main actors of the country's cyber protection and to provide the tools to understand its functioning, in the light of the innovation constituted by the recent completion of the National Cyber Security Perimeter.

In line with the objectives of ERACLITO, which is to provide tools to facilitate the compliance of perimeter subjects, much space will be devoted to the security perimeter and its procedures. The technical aspects of compliance work for Perimeter subjects are elaborated upon in appendix I, which complements this analysis.

The examination of the national security infrastructure is divided into two parts. Paragraph

---

<sup>530</sup> Please refer to Giusella Finocchiaro, 'Una Prima Lettura Del Reg. UE n. 910/2014 (c.d. "Eidas"): Identificazione "on Line", Firme Elettroniche e Servizi Fiduciari (Reg. UE n. 910/2014)', *Le Nuove Leggi Civili Commentate*, no. 3 (2015): 419–28; Anna Lazzaro, 'Informazione e Comunicazione Digitale Nel Processo Di Modernizzazione Della Pubblica Amministrazione', *MediaLaws - Law and Policy of the Media in a Comparative Perspective*, no. 2 (2018): 11; Juan Francisco Rodriguez Ayuso, 'Verso il raggiungimento di un mercato unico interno in materia di transazioni elettroniche. Il nuovo regolamento europeo 910/2014', *Federalismi.it*, no. 24 (2017): 14.

<sup>531</sup> The recent success of generative artificial intelligence brings with it a host of new problems, one of which is the processing of data generated by conversations with models. This information can be used to profile users and to re-tune the model, which could be trained to give answers that are biased towards certain ideological or political sides. The issue of bias and the danger of the tool returns, especially in the run-up to the elections. See Licia Califano, 'Chat GPT e Meta ["Meta Platforms Ireland Limited" - MPIL] EDI ["Election Day Information"]': Spunti Problematici Su Profili Regolatori e Ruolo Delle Autorità Di Controllo Di Protezione Dati', *Federalismi.it*, no. 10 (2023): 4–15; Antonio Palmieri, 'Intelligenza artificiale ed operazioni di trattamento dei dati personali', *Il Foro italiano*, no. 3 (2023): 210–12.

<sup>532</sup> Mark Cole and Sandra Schmitz, 'The Interplay Between the NIS Directive and the GDPR in a Cybersecurity Threat Landscape', *SSRN Electronic Journal*, 2019, <https://doi.org/10.2139/ssrn.3512093>.

IV.1, is devoted to developments prior to the Security Perimeter. Paragraph IV.2 is dedicated to the Perimeter and its implementing acts to help reconstructing its logics. This will lead to the extraction of the functional requirements from the Perimeter legislation in the appendix I.

#### IV.1 The Perimeter before the Perimeter

Having said that, it is good to try to outline the first interventions that helped to lay the foundations of the current cybersecurity framework.

A common root can be found in the digitisation process of the country, which started in the 1990s with the first computerisation of the public administration. If at first the aim was to automate processes, then the issue of simplifying the relationship with the citizen followed. In 2005, the Digital Administration Code (in Italian the so-called *Codice dell'Amministrazione Digitale* or CAD) enshrined for the first time the right to address the public administration by means of digital tools. In terms of the affirmation of rights, the next milestone was the Digital Citizenship Charter (in Italian *Carta della Cittadinanza digitale*), which regulates the new relationship between administration and citizen<sup>533</sup>.

At the same time, digitalisation was accompanied by an increase in cybercrime. In the same year, Italy set up the National Cybercrime Centre for the Protection of Critical Infrastructure (in Italian *Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche* or CNAIPIC)<sup>534</sup>.

The increase in security incidents had led to the creation of an initial organisational structure to collect information and support mitigation and response activities. The implementation of European directives reforming the electronic communications system had prompted the introduction of a first obligation to report security incidents to the Ministry of Economic Development, where the national Computer Emergency Response Team (CERT) was based<sup>535</sup>. This was to serve as a coordinating body for the network of national CERTs, including the one for public administration. After several transformations, the creation of the Agency for Digital Italy (in Italian *Agenzia per l'Italia Digitale* or AgID) led to the creation of

---

<sup>533</sup> Legislative Decree 2017 of 13 December 2017 introduced the Charter of Digital Citizenship (Section II) into Chapter I of the CAD. The new section enumerates the rights of citizens and companies vis-à-vis the administration, thus configuring a true e-government. The AgID guidelines, based on article 71 of the CAD, are the instrument for the effective implementation of these rights. Please consult Bruno Carotti, 'Il Correttivo al Codice Dell'amministrazione Digitale: Una Meta-Riforma', *Giornale Di Diritto Amministrativo*, no. 2 (2018): 131–41; Francesco Martines, 'La Digitalizzazione Della Pubblica Amministrazione', *MediaLaws*, no. 2 (2018): 10.

<sup>534</sup> The CNAIPIC was introduced by Decree Law 144 of 27 July 2005, converted with amendments by Law 155 of 31 July 2005, and by the Decree of the Ministry of the Interior of 9 January 2008 (Identification of Critical Information Infrastructures of National Interest). The formal establishment took place with the decree of the Chief of Police of 7 August 2008.

<sup>535</sup> Reference is made to Article 16-bis of Legislative Decree 259 of 2003 (the so-called Electronic Communications Code), as introduced by Legislative Decree 70 of 28 May 2012, which transposed Directive 2009/140/EC on electronic communications networks and services and Directive 2009/136/EC on the processing of personal data and the protection of privacy. Article 16a was recently repealed following the transposition of European Directive (EU) 2018/1972, establishing the European Electronic Communications Code, but its general meaning remained intact. Already in 2012, the transposition had introduced, on the one hand, the obligation to adopt technical and organisational measures identified by the Ministry of Economic Development to ensure the security of electronic communications networks and services. On the other hand, the obligation to notify the Ministry of any significant breach of security or loss of integrity. For a comparison with the European legislation on electronic communications, see the paragraph. III.1.1.1.

CERT-PA<sup>536</sup>.

CERT-PA, but more generally the whole issue of cybersecurity in public administration, was the cornerstone of the Digital Growth Strategy 2014-2020. “The territorial analysis still showed a delay in the implementation of systems to protect digital infrastructures and services, and the need to prevent cybercrime problems”<sup>537</sup>. It was necessary to invest in security, and AgID was given the task of developing standards and guidelines for public administration. A wide range of enablers for digitisation needed attention, from transaction security to the security of justice and public infrastructure, such as healthcare or digital identity.

These needs were reflected in the identification of minimum ICT security measures for public administrations, to be adopted by 31 December 2017, and in various guidelines prepared and made available by AgID<sup>538</sup>. These included the guidelines for the development and definition of the network of regional CERTs<sup>539</sup>.

The latest three-year plan for IT in public administrations highlights the urgent need to consolidate an infrastructure plan focused on interoperability and the re-use of public data. It is not only a question of centralising services, but also of emphasising the use of the cloud, which must become the key tool for combining security and interoperability, providing control and audit tools for smaller public administrations.

Despite the efforts made, it should be noted that security objectives still need to raise awareness of cyber risks. The lack of risk awareness goes hand in hand with the lack of local

---

<sup>536</sup> Over time, several public bodies have been set up to oversee the digitisation of public administration. The first was the Authority for Information Technology in Public Administration (in Italian *Autorità per l'informatica nella pubblica amministrazione* or AIPA), established by Legislative Decree 39 of 12 February 1993. It was later replaced by the National Centre for IT in Public Administration, on the basis of Article 176 of Legislative Decree 196 of 30 June 2003 (the so-called Privacy Code). A further step followed with the creation and replacement of the National Board for the Digitisation of Public Administration (in Italian *Ente nazionale per la digitizzazione della pubblica amministrazione* or DigitPA) by Legislative Decree 177 of 1 December 2009. The final organisation was achieved with the abolition of DigitPA and the creation of AgID. See articles 19 and 22 of Legislative Decree 83 of 22 June 2012, converted by Law 134 of 7 August 2012. See also Tazio Bianchi, ‘Firma Digitale e Ruolo Dell’Aipa Alla Luce Del d.lgs. 23 Gennaio 2002, n. 10’, *Cyberspazio e Diritto*, no. 1 (2002): 1–7; Renata Carpentieri, ‘L’Agenda Digitale Italiana’, *Giornale Di Diritto Amministrativo*, no. 3 (2013): 225–33; Carlo Notarmuzi, ‘DigitPA: La Terza Riorganizzazione Dell’informatica Pubblica’, *Giornale Di Diritto Amministrativo*, no. 10 (2010): 1014–20; Vittorio Zambrano, ‘Il Nuovo Capitolato AIPA.’, *Enti Pubblici*, no. 2 (1997): 149–67.

<sup>537</sup> My translation from Agenzia per l’Italia digitale, ‘Strategia per la Crescita Digitale 2014-2020’, 3 March 2015, 58, [https://www.agid.gov.it/sites/default/files/repository\\_files/documentazione/strategia\\_crescita\\_digitale\\_ver\\_def\\_21062016.pdf](https://www.agid.gov.it/sites/default/files/repository_files/documentazione/strategia_crescita_digitale_ver_def_21062016.pdf).

<sup>538</sup> Consider the guidelines for secure software development. Please refer to Agenzia per l’Italia digitale. ‘Linee Guida Sviluppo Software Sicuro’, 21 November 2017. [[https://www.agid.gov.it/sites/default/files/repository\\_files/documentazione/lineeguidasicurezza-introduzione.pdf](https://www.agid.gov.it/sites/default/files/repository_files/documentazione/lineeguidasicurezza-introduzione.pdf)]([https://www.agid.gov.it/sites/default/files/repository\\_files/documentazione/lineeguidasicurezza-introduzione.pdf](https://www.agid.gov.it/sites/default/files/repository_files/documentazione/lineeguidasicurezza-introduzione.pdf)). Although this is not the context to go into detail, the importance of the AgID guidelines represented a restructuring of the system of sources, configuring a new relationship between law and technology. See also Pietro Falletta, ‘Le Linee Guida Dell’Agenzia per l’Italia Digitale’, *Giornale Di Diritto Amministrativo*, no. 2 (2021): 163–71.

<sup>539</sup> The introduction was intended to reduce the workload of the CERT-PA and to create intermediary levels in the relationship with the local public administration. See also Agenzia per l’Italia digitale, ‘Linee guida per lo sviluppo e la definizione del modello nazionale di riferimento per i CERT regionali’, 13 February 2020, <https://docs.italia.it/AgID/documenti-in-consultazione/lg-cert-regionali/it/bozza/index.html>.

organisational structures capable of effectively preparing for and responding to incidents<sup>540</sup>.

It calls for a holistic approach to cybersecurity, capable of harnessing resources within the public structure and ensuring the affirmation of a fifth generation of fundamental rights<sup>541</sup>.

#### IV.1.1 History and foundations of the Italian secret service system

While there is no doubt that the efforts dedicated to the security of the public administration and its interoperability were a fundamental intermediate step in the initial management of cybersecurity, it must be recognised that these efforts alone did not constitute an organic system.

Not surprisingly, the real and direct foundations of the current cybersecurity architecture are to be found in the system for the security of the Republic. The Italian intelligence services have an ancient and contrasting history, rooted in the Unification. Their development has followed the decline of the State during the war years and then the development of the Republic in all its phases.

Although the subject of services could lead to much broader discussions<sup>542</sup>, it is of interest here to briefly outline the steps that led to the current system. The focus should be on the system level and the structure of the operation in order to describe the introduction of the first cybersecurity competences.

At the outset of this reorganisation, it is important to emphasise its military origins. The birth of the secret services can be historically traced back to 1854, with the creation of the secret service of the Ministry of Foreign Affairs, which was soon joined by full-fledged military secret services. However, the activity of the services was not confined to military bodies.

Italian history has seen a succession of specialised bodies within various ministerial institutions, operating in a scattered and fragmented way, not without overlaps and duplications<sup>543</sup>.

---

<sup>540</sup> Agenzia per l'Italia Digitale and Dipartimento per la Trasformazione Digitale, 'Piano Triennale per l'informatica nella Pubblica Amministrazione 2020-2022', July 2020, [https://www.agid.gov.it/sites/default/files/repository\\_files/piano\\_triennale\\_per\\_l\\_informatica\\_nella\\_pa\\_2020\\_2022.pdf](https://www.agid.gov.it/sites/default/files/repository_files/piano_triennale_per_l_informatica_nella_pa_2020_2022.pdf).

<sup>541</sup> See Antonio Iannuzzi and Francesco Laviola, 'I Diritti Fondamentali Nella Transizione Digitale Fra Libertà e Uguaglianza', *Diritto Costituzionale*, no. 1 (2023): 9–40. The authors question the adequacy of the current constitutional framework for affirming citizens' fundamental digital rights. A teleological reading of the Constitutional Charter in the light of European law is proposed. The same concept is widely discussed in the latest scientific debate. See Oreste Pollicino, 'Di Cosa Parliamo Quando Parliamo Di Costituzionalismo Digitale?', *Quaderni Costituzionali*, no. 3 (2023): 569–94; Tommaso Edoardo Frosini, 'L'ordine Giuridico Del Digitale', *CERIDAP*, no. 2 (2023): 36–65; Valentina Cavanna, 'Nuovi Poteri, Vecchi Problemi. Il Costituzionalismo Alla Prova Del Digitale', *Diritto Pubblico Comparato Ed Europeo*, no. 1 (2023): 223–48; Erik Longo and Andrea Pin, 'Oltre Il Costituzionalismo? Nuovi Principi e Regole Costituzionali per l'era Digitale', *Diritto Pubblico Comparato Ed Europeo*, no. 1 (2023): 103–16; Alessandro Sterpa, 'L'ordine giuridico dell'algoritmo: un nuovo ordinamento giuridico', in *L'ordine giuridico dell'algoritmo*, Tiresia - Future Studies and Law 1 (Naples: Editoriale Scientifica, 2024), 9–31, [https://editorialescientifica.it/wp-content/uploads/2024/04/Open-access-Sterpa\\_Lordine-giuridico-dellalgoritmo.pdf](https://editorialescientifica.it/wp-content/uploads/2024/04/Open-access-Sterpa_Lordine-giuridico-dellalgoritmo.pdf).

<sup>542</sup> Just as an example, consider the question of the constitutional basis of intelligence activity. Please refer to Silvano Labriola, 'Informazioni per La Sicurezza e Segreto Di Stato.', *Diritto e Società* 2, no. 4 (1981): 833–59. On the basis of these foundations, the profiles of the relationship between the services and the judicial authority, especially with regard to the imposition of state secrecy, and the system of parliamentary control are no less relevant.

<sup>543</sup> Historical sources indicate that there were at least six intelligence services at the time of unification. The most important of these were within the Ministry of the Interior and the Diplomatic Service. See A. Massera and



Leaving aside the details of the countless steps that have shaped the institutional profile of the services, it is possible to grasp the remarkable complexity that emerges from the historical data. Until the 1970s, intelligence activities were carried out both by the secret services in the strict sense and by the public security apparatuses<sup>544</sup>. This marked fragmentation had led to a negative perception of the work of the intelligence services, which were often associated with activities that were not in line with the interests of the Community state<sup>545</sup>.

Given the diversity of actors using intelligence techniques, even inappropriately, the common identification of the activity with that of the armed forces remained. This idea was supported not only by historical reasons, but above all by the different equipment of the military apparatus compared to its civilian counterparts. The greater resources and manpower available to the military have often led to an expansionist tendency, often justified by the lack of a formal legal basis for intelligence activities carried out by civilian agencies<sup>546</sup>.

"The government, in exchange for the support and cover it received (or rather that it thought it received [...]) from the military apparatus [...] ended up abdicating, in fact, even that role of supervision and general direction that the system had assigned to it. In this way, the security services became increasingly configured as a separate structure between separate bodies, with the effect that the security services [...] ended up interfering more and more in the political sphere"<sup>547</sup>.

In this context, the Constitutional Court issued a historic ruling on the issue of state secrecy in criminal proceedings. On the basis of this milestone, the first legislative restructuring of the sector was established<sup>548</sup>.

---

C. Mosca, 'I servizi di informazione', in *Trattato di diritto amministrativo, pt. spec.*, ed. S. Cassese, vol. I (Milano, Italy, 2003), 520.

<sup>544</sup> Massera and Mosca, 522. The authors reconstruct with great precision the main steps in the evolution of the Italian secret services up to the 1970s. For details, please refer to the full text, but here are just some of the main sources that preceded the first organic reform of the sector. For example, Royal Decree Law no. 1909 of 15 October 1925, which established the Military Intelligence Service under the Chief of the General Staff, is one of the first relevant sources. After decades of vagueness, Legislative Decree No. 955 of 21 April 1948 formally assigned the coordination of intelligence activities to the Chief of Defence Staff. The delegated law no. 1862 of 12 December 1962, by presidential decree no. 1477 of 18 November 1965, had confirmed this position by reaffirming the supervision of the Chief of Defence Staff over the Armed Forces Intelligence Service. In 1966, SIFAR was renamed the Defence Intelligence Service (in Italian Servizio informazioni difesa, SID). On the Ministry of the Interior side, there were no minor changes. After several institutional and name changes, a Security Intelligence Service (in Italian Servizio informazioni sicurezza, SIS) was established in the 1970s.

<sup>545</sup> See G. Cocco, 'Vicende Storiche e Deviazioni Dei Servizi Di Informazione e Di Sicurezza', in *I Servizi Di Informazione e Di Sicurezza Nell'ordinamento Italiano* (Padova, Italy, 1980), 174–83. The author identified three main types of 'deviations'. The first can be traced back to the normal actions of the services, a second is a symptom of disorder in the internal behaviour of the services and a third is an expression of a contradictory tendency towards representative institutions. See the chapter for details.

<sup>546</sup> G. Cocco, 'Modi e Forme Di Esercizio Dell'attività Informativa e Di Sicurezza Nel Regime Precedente La L. 24 Ottobre 1977, N. 801', in *I Servizi Di Informazione e Di Sicurezza Nell'ordinamento Italiano* (Padova, Italy, 1980), 102–5. The author recalls that, unlike the military services, the civilian services had no explicit basis for their activities. On the contrary, the supervision of the Armed Forces Intelligence Service by the Chief of Defence Staff was confirmed by Presidential Decree No. 1477 of 18 November 1965, implementing Delegated Act No. 1862 of 12 December 1962.

<sup>547</sup> My translation from S. Labriola, *Le Informazioni per La Sicurezza Dello Stato* (Milano, Italy, 1978).

<sup>548</sup> Reference is made to Judgement No. 86 of 24 May 1977. The constitutional basis for the institution of the State Secrets had already been placed in the "supreme interest of the security of the State in its international

With Law 801 of 1977, the Italian legislator had given the subject of the secret services its first organic discipline, at the same time incorporating the indications of the Constitutional Court. Until then, their activities had operated “outside the democratic circuit and outside an organic legislative framework, in derogation of the principle of legality”. The matter was thus removed from the “infra-constitutional dimension of opacity and irresponsibility in which it had been fluctuating”<sup>549</sup>.

Two services were created: the Military Intelligence and Security Service (in Italian *Servizio per le informazioni e la sicurezza militare* or SISMI) in the Ministry of Defence, and the Intelligence and Democratic Security Service (in Italian *Servizio per le informazioni e la sicurezza democratica* or SISDE) in the Ministry of the Interior. The President of the Council of Ministers has been entrusted with “the overall direction, political responsibility and coordination of information and security policy”, which he exercises by means of directives and provisions on organisation and coordination<sup>550</sup>. Despite the centrality of its role, it should be noted, in accordance with the Constitutional Court's dictate, that there was no real relationship of direct dependence between the Services. Each of them was obliged to inform the Minister of reference, with whom there was a relationship of absolute dependence. Consequently, the fact that the President of the Council of Ministers had the information activity of the Executive Committee for the Intelligence and Security Services (in Italian *Comitato esecutivo per i servizi di informazione e sicurezza* or CESIS), set up under the Presidency of the Council of Ministers to coordinate the activities of the two services, was mitigated by the need to channel impulses through the Ministers of Defence and of the Interior. This need was partially alleviated by the inclusion of both Ministers among the members of the Interministerial Committee for Information and Security (in Italian *Comitato interministeriale per le informazioni e la sicurezza* or CIIS). The picture was completed by the strengthening of the role of parliamentary control, a privileged forum in which to decide on

---

personality, i.e. the interest of the State-community in its own territorial integrity, in its own independence and, at the limit, in its very survival” (Constitutional Court, Judgement No. 82 of 14 April 1976). On this conceptual basis, the doctrinal debate has also found fertile ground. See among others Labriola, ‘Informazioni per La Sicurezza e Segreto Di Stato.’; Luciano Mauriello, ‘Libertà, Attività Informativa e Sicurezza Dello Stato.’, *Nuova Rassegna Di Legislazione, Dottrina e Giurisprudenza*, no. 15–16 (1987): 1579–96. Recognising the constitutional nature of national security, the Court had approached the issue as a balancing of fundamental rights. The Court had declared Articles 342 and 352 of the Code of Criminal Procedure partially unconstitutional in two different respects. Firstly, the final decision on secrecy must be taken by the President of the Council of Ministers, since activities relating to national security must be decided by the head of state. According to Article 95(1) of the Constitution, the Prime Minister “shall direct and be responsible for the general policy of the Government”. This includes the highest political activity, that of the external and internal defence of the State. In this sense, since the decision to affix secrecy takes on an exquisitely political character, the limitation of judicial review is balanced by the political control exercised by Parliament. In this sense, the power of the Government is not unchecked, but its responsibility lies in its natural seat, that of Parliament. Notwithstanding this premise, the President's decision to confirm secrecy must always be motivated, at least with an indication of the “essential reasons”. Please see the comments of Adele Anzon, ‘Interrogativi Sui Riflessi Sostanziali Della Nozione Di Segreto Di Stato Individuata Dalla Corte Costituzionale’, *Giurisprudenza Costituzionale*, no. 4–6 (1977): 866–69; Paolo Pisa, ‘Il Segreto Di Stato Di Fronte Alla Corte Costituzionale: Luci Ed Ombre In Attesa Della “Riforma”’, *Giurisprudenza Costituzionale*, no. 8 (1977): 1206–14; Aldo Maria Sandulli, ‘Note Minime in Tema Di Segreto Di Stato’, *Giurisprudenza Costituzionale*, no. 8 (1977): 1200–1205.

<sup>549</sup> Mario Savino, ‘Solo per i Tuoi Occhi? La Riforma Del Sistema Italiano Di Intelligence’, *Giornale Di Diritto Amministrativo*, no. 2 (2008): 123.

<sup>550</sup> The President of the Council of Ministers was given the power of direction and political responsibility over the bodies of the service system. See Article 1 of Law 801 of 1977.

the President's responsibility, particularly with regard to the application of state secrecy. The sensitivity of the subject had led the legislator to create a special parliamentary control committee, the Parliamentary Control Committee on Intelligence Services (in Italian *Comitato parlamentare di controllo sui servizi segreti* or COPACO), which could exercise a supervisory role over the activities of the services and was informed by the President of all cases of objection to secrecy<sup>551</sup>.

If, on the one hand, the law had the merit of legalising the work of the secret services<sup>552</sup>, on the other hand it had initiated a process of transferring this function from the military to the civilian sphere. This latter process would have required other subsequent interventions in order to be fully implemented, due to the already mentioned differences in the equipment of the reference administrations. Despite the good intentions of the legislator, this fundamental difference in the initial conditions of the two apparatuses continued to affect the relations between the two spheres of competence. The civilian apparatus continued to operate under the protection of the military apparatus<sup>553</sup>. For the sake of brevity, we shall refrain from a detailed analysis of the operational discipline and structure introduced by Law 801 of 1977, which is outlined in Figure 19<sup>554</sup>.

---

<sup>551</sup> Parliament was to receive a six-monthly written report from the government on the activities of the services. In addition, COPACO could request information on the main lines of the structures and activities of the services. If, following the request for information, the President of the Council of Ministers objected to state secrecy, the Committee could decide, by an absolute majority, to report to each House. The same mechanism applied to cases of secrecy before the judiciary, but a unanimous vote of the committee was required. See Articles 11-17 of Law 801 of 1977.

<sup>552</sup> At the same time, the special nature of their status remained, to the extent that the Council of State defined them as "autonomous administrative offices". See Council of State, Section IV, 3 February 1998, No. 162.

<sup>553</sup> The Figure 19 confirms this practice, also because of the closer relationship between the SISMI and the Operational and Situational Intelligence Services (SIOS) existing in each Armed Forces or State Armed Corps. In total, there were four SIOS in the Army, the Navy, the Air Force and the Carabinieri Corps. Although they only performed military technical and military police tasks, they had to act in close liaison with the SISMI. Since 1997, this fragmentation has been eliminated with the creation of the Information and Security Department (RIS) within the General Staff of the Armed Forces. This privileged relationship with military intelligence undoubtedly increased its scope and importance.

<sup>554</sup> Simply refer to G. De Liutiis, *Storia Dei Servizi Segreti in Italia* (Roma, Italy, 1985); Massera and Mosca, 'I servizi di informazione'; A. Viviani, *Servizi Segreti Italiani 1815/1985* (Roma, Italy, 1985).

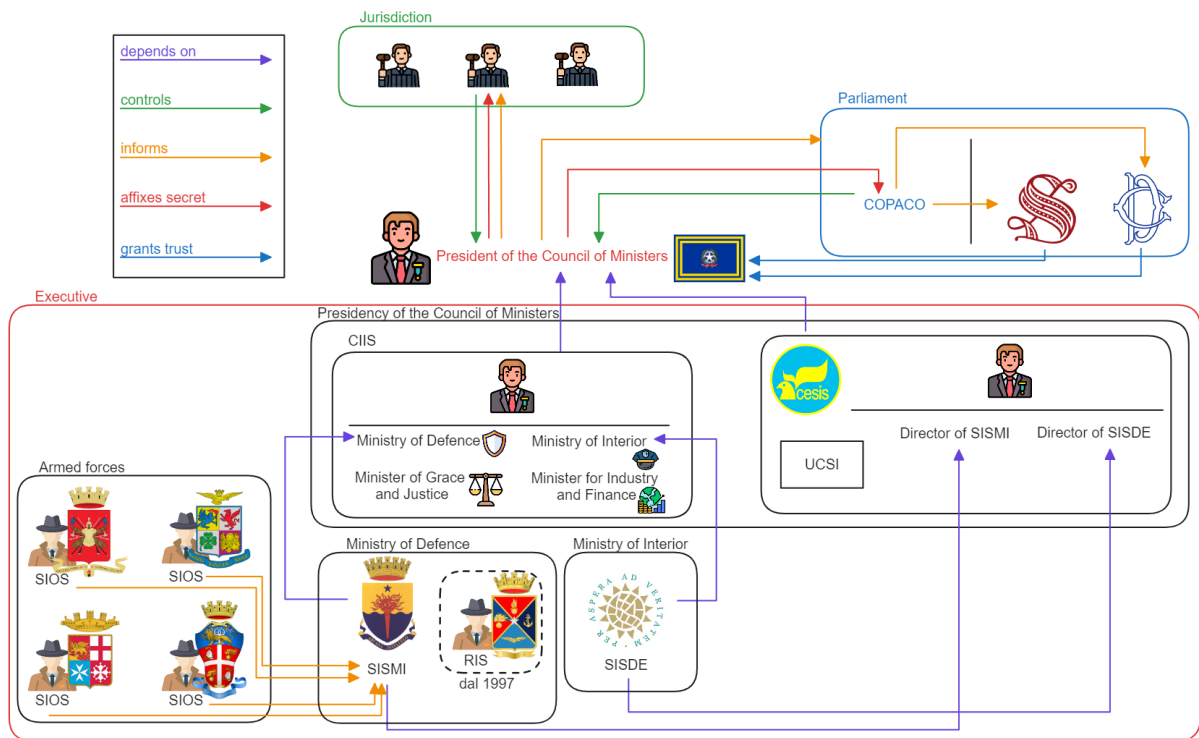


Figure 19 - Italian Intelligence before Law n. 124/2007

#### IV.1.2 The law n. 124 of 2007

On the basis of these brief remarks, it is possible to define the impact of the recent reform of the intelligence system on the security of the Republic.

After several unsuccessful attempts at reform<sup>555</sup>, the legislature had intervened to complete the process of bringing the Services into the sphere of legality that had begun in the 1970s. Law 801 of 1977 itself contained, without too much ambiguity, an explicit denunciation of its provisional nature, as understood by the doctrine<sup>556</sup>. Despite this initial intention, the provisional nature of the legislation continued for more than thirty years, until the approval and entry into force of Law 124 of 2007. This opened the way to an organic reform of the subject, which concerned the structure, organisation and functions of the security intelligence system, without neglecting parliamentary control. The process had required several successive interventions due to the numerous references to the source of the legislation, until

<sup>555</sup> Three attempts at reform prior to Law 124/2007 can be recalled here. The Ciampi bill (A.S. 1628), the D'Alema-Mattarella bill (A.S. 4162) and the Berlusconi bill (A.S. 1513). While the first two would have represented organic reforms of the system, the Berlusconi bill would have limited itself to intervening in some critical points of the previous legislation, which would thus not have been overcome. Of particular interest was the proposal of the Ciampi government, which aimed to overcome the dualistic model of the intelligence services by introducing a single structure centralised in the Presidency of the Council of the Ministers. The domestic and foreign subdivisions would have remained, but within two departments within the new structure, which would have remained conceptually unitary. See for an overview of the pre-reform legislation. See Vittorio Stelo, 'Così è Cambiata l'Intelligence in Italia', *Gnosis*, no. 4 (2007), <https://gnosis.aisi.gov.it/Gnosis/Rivista13.nsf/ServNavig/59>.

<sup>556</sup> Article 18 began by indicating the correct reference for criminal cases still referring to international internal political secrecy, at least "until the date of the enactment of a new organic law on the subject of secrecy". See Piero Luigi Vigna, 'La Nuova Disciplina Dei Servizi Di Sicurezza', *La Legislazione Penale*, no. 4 (2007): 693–702.

which the previous regime had continued to apply in prorogation<sup>557</sup>.

The first fundamental innovation is to be found in the strengthening of the central role of the President of the Council of Ministers, by confirming the atypical mixture of powers inaugurated in the 1970s. The reference is to that particular centralisation of both political and administrative policy-making powers which had led the doctrine to define the figure of the "President-Minister"<sup>558</sup>. The highest leadership, the overall responsibility for security information policy and the imposition of state secrecy are flanked by more penetrating powers of financial allocation<sup>559</sup> and, above all, powers of appointment.

Whereas previously the Services were dependent on the Minister of the Interior and the Minister of Defence, who had the power to appoint the Director, the process of centralisation abolished this indirect dependence and gave the appointment to the President of the Council of Ministers<sup>560</sup>. The two ministers share a residual functional and organisational dependency, which is expressed in their participation in the Interministerial Committee for the Security of the Republic (in Italian *Comitato Interministeriale per la Sicurezza della Repubblica* or CISR), the successor to the CIIS. This committee, which is attached to the Presidency of the Council of Ministers, now acts as the main planning body for the Republic's security policy<sup>561</sup>. It draws up the general guidelines and fundamental objectives of the security information policy. It also has the power to advise on the President of the Council's decisions on the allocation of financial resources<sup>562</sup>.

Another major restructuring took place in the Presidency of the Council of Ministers. The simple structure of CESIS was replaced by the Department of Security Intelligence (in Italian

---

<sup>557</sup> See Articles 4(7), 6(10), 7(10), 21(1) and 29(3) of Law 124 of 2007. In addition to the reference to regulations, several other "atypical" secondary sources have intervened to complete the system. The President of the Council Decrees on the management of classified information come to mind. By way of example, reference is made here to:

- D.P.C.M. of 8 April 2008 ("Criteria for identifying news, information, documents, acts, activities, things and places that may be subject to state secrecy");

- D.P.C.M. no. 7 of 12 June 2009 ("Determination of the scope of the individual levels of secrecy, the subjects subject to classification, the criteria for identifying the subjects subject to classification, as well as the methods of access to military sites or sites defined as being of interest for the security of the Republic").

- D.P.C.M. no. 4 of 22 July 2011 ("Provisions on the administrative protection of state secrets and classified information");

- D.P.C.M. of 6 November 2015, no. 4 ("Provisions on the digital signature of classified documents");

- D.P.C.M. of 6 November 2015, No. 5 ("Provisions for the administrative protection of State secrets and classified information and exclusive disclosure"), as updated by the subsequent D.P.C.M. of 2 October 2017, No. 3.

For further information on regulatory interventions within the information system for the security of the Republic, please visit the following website 'Normativa Di Riferimento - Sistema Di Informazione per La Sicurezza Della Repubblica', accessed 1 January 2024, <https://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento.html>.

<sup>558</sup> Labriola, *Le Informazioni per La Sicurezza Dello Stato*, 124.

<sup>559</sup> In addition to the power to allocate resources between the two services, there is also the power to determine the allocation between ordinary and reserved funds. See article 29 par. 2 of law 124 of 2007.

<sup>560</sup> See Article 1 par. 1 of Law 124 of 2007 for an overview of the powers of the President of the Council of Ministers.

<sup>561</sup> Vigna, 'La Nuova Disciplina Dei Servizi Di Sicurezza', 697.

<sup>562</sup> See Article 5 of Law 124 of 2007.

*Dipartimento delle Informazioni per la Sicurezza* or DIS), which is a particularly complex body with multiple functions. On the one hand, it is responsible for coordinating the two Services, although it is not a hierarchically superior body. The DIS must be kept constantly informed of the activities of the Services, which must give it access to their reports so that it can draw up comprehensive analyses to be submitted to the CISR. This information role must not be understood as a recourse to the information system for the security of the Republic, since the aim is to provide the greatest possible benefit to the country. For this reason, a permanent exchange of information with the police forces and the public administration must be facilitated by means of appropriate reports<sup>563</sup>. The President of the Council of Ministers, in particular, must be able to benefit from this virtuous circle of information. The optimal exercise of presidential powers is perhaps the primary objective of this structure, which depends directly on the President himself.

The replacement of CESIS was also an opportunity to renew the administrative support structure. The DIS has a number of offices within it to support the fulfilment of its functions. Among these is the Central Office for Security (in Italian *Ufficio Centrale per la Segretezza* or UCSe), which has replaced the UCSI (in Italian *Ufficio centrale per la sicurezza*) in the task of issuing authorisations to handle classified information. It is supported by the Central Archives Office and the Training School. The former is responsible for the exclusive preservation of documents relating to the activities and budgets of the agencies, as well as documents relating to the application of functional guarantees. The Training School, on the other hand, was created to ensure the training, education and updating of DIS, AISE and AISI staff.

The most significant innovation, however, is the creation of a Special Inspectorate within the DIS. Historically, the function of controlling the services has always been assigned on the one hand to Parliament, which is the most appropriate forum for resolving questions concerning the political actions of the Prime Minister, and on the other hand to the criminal justice system. The 2007 reform created a third type of control, internal to the system of the services. Consequently, the coordinating role of the DIS also fulfils a control role. Subject to the restriction of not interfering with ongoing operations, the control of the inspectors is very penetrating, as state secrecy cannot be imposed on subjects internal to the intelligence system for the security of the Republic<sup>564</sup>.

The direct control of the services and the support of an effective information system have contributed to strengthening the centrality of the figure of the Prime Minister, whose powers are more strictly defined. In particular, the practice of appointing a delegated authority is specifically regulated. Whereas previously most of the President's powers were delegated to the Secretary General of CESIS, the new wording introduces some restrictions on the possibility of delegation. Firstly, not all of the President's powers can be delegated, but only those which are not exclusively his. No less important, the delegated authority must be a political body, i.e. an undersecretary of state or a minister without portfolio. Nevertheless, delegation is always optional, since the President is free to retain all his functions or to take them on himself in case of need<sup>565</sup>.

Having established this premise about the bodies that support the information system for the security of the Republic, let us turn our attention to the new organisation of the Services.

---

<sup>563</sup> See Article 4 of Law 124 of 2007.

<sup>564</sup> See Article 4 c. 8 of Law 124 of 2007.

<sup>565</sup> See Article 3 of Law 124 of 2007.

The binary system that has always characterised Italian history does not disappear. The former SISMI and SISDE are replaced by the AISI and the AISE, which are set up as independent administrative agencies, essentially as first-level offices independent of the ministerial apparatus and with a certain degree of operational autonomy in the implementation of government guidelines. While this aspect is new only from a formal point of view, the real innovation lies in the criterion of the distribution of competences. Whereas SISMI and SISDE had clear competences according to subject<sup>566</sup>, AISI and AISE have an action defined according to a territorial criterion<sup>567</sup>.

There is a complete equalisation of competences, mediated by the attribution to the AISI of action within the territory of the Republic and to the AISE of action outside it. This solution compensates for the historical predominance of the military apparatus over the civilian one, made possible also by the ambiguity of the wording of the competences attributed to the two agencies. At the same time, the exclusivity of intelligence functions was established in order to avoid the emergence of a multiplicity of atypical bodies, particularly within the armed forces. For this reason, the legislator had explicitly sanctioned the RIS's independence from the intelligence system. In this context, there was an opaque selection system that exempted the rule of public competition. The reform also addressed this shortcoming by restoring uniformity in relation to the other administrations.

When dealing with the main actors within the information system for the security of the Republic, the counterweights of the information system cannot be overlooked. As mentioned above, the current system is based on three pillars. In addition to the DIS, there are the constraints arising from the relationship with other powers.

As far as the judiciary is concerned, the critical aspect in which the reform intervened was that of state secrecy. Whereas in the past this was the only instrument of protection for officials obliged to perform criminal acts<sup>568</sup>, it was accompanied by a regulation on functional

---

<sup>566</sup> Article 4 of Law 801 of 1977 assigned to the SISMI all "intelligence and security tasks for the military defence of the independence and integrity of the State against any danger, threat or aggression". Article 6, on the other hand, assigned to the SISDE "intelligence and security tasks for the defence of the democratic State and the institutions established by the Constitution as its foundations, against anyone who attempts to do so and against any form of subversion".

<sup>567</sup> Although Articles 6 and 7 of Law 124 of 2007 refer to a very similar formulation of competences to the previous legislation, in both cases reference is made to intelligence activities for security purposes, carried out inside and outside the territory of the Republic respectively. The basis of this activity is attributed to the political, military, economic, scientific and industrial interests of Italy, an extremely abstract and vague formulation.

<sup>568</sup> The reference article, later expanded and amended by Law 124 of 2007, is Article 202 of the Criminal Code, which regulates the imposition of state secrecy in the event that the testimony of a witness relates to information covered by state secrecy. The President of the Council of Ministers is asked by the criminal court to confirm the existence of the secret within 60 days of the request. If the secrecy is confirmed, the judge may not compel the witness to testify about these facts. If the information is essential, it must be declared inadmissible on the grounds of secrecy. The only further remedy in these situations is the conflict of powers before the Constitutional Court, which is the only judicial body before which the state secret cannot be invoked. Nazzareno Tirino, 'Segreto di Stato e conflitto di attribuzione fra poteri dello Stato', *dirittifondamentali.it*, no. 1 (2016), [http://dirittifondamentali.it/wp-content/uploads/2019/04/1\\_2016-tirino\\_segreto-di-stato-e-conflitto-di-attribuzione-fra-poteri-dello-stato.pdf](http://dirittifondamentali.it/wp-content/uploads/2019/04/1_2016-tirino_segreto-di-stato-e-conflitto-di-attribuzione-fra-poteri-dello-stato.pdf). The same mechanism can be found in Article 256 on the duty of disclosure. Undoubtedly, the issue raises delicate questions regarding the balance between security and individual freedoms. The infamous Abu Omar case is an example of this fragile balance, which highlighted the contrast between the Italian Constitutional Court and the EDU Court. As this is not the place for a topic that would require a more in-depth discussion, please refer to Tommaso F. Giupponi, 'La Corte e Il Segreto: Abu Omar, Ultimo Atto', *Quaderni Costituzionali*, no. 2 (2014): 386–89; Alessandro Pace, 'Stato Costituzionale e

guarantees. The idea is to provide protection for the conduct of agents by introducing a special justification for their conduct if it is duly authorised. This has helped to reduce the use of state secrecy, which has been made more restrictive both by specifying typical acts and by limiting its duration to 15 years<sup>569</sup>.

However, the most appropriate forum for scrutinising the Prime Minister's actions, including decisions concerning the secret services, remains Parliament. The former parliamentary committee, COPACO, was replaced by the Parliamentary Committee for the Security of the Republic (COPASIR). Although its task is still to verify systematically and continuously that the activities of the secret services are carried out in accordance with the Constitution and the laws, in the exclusive interest and for the defence of the Republic and its institutions<sup>570</sup>, the reform led to a strengthening of its functions and powers of control.

The number of people who can be summoned to a hearing was increased, in addition to members of the Security Information System. Employees of the Services may also be heard, as well as any other person who can provide useful information. The same extension was made for the production of documents relating to ongoing proceedings or investigations by judicial authorities or parliamentary inquiries. Documents may also be requested from members of the services or public administration bodies, subject to the defence of confidentiality equivalent to State secrecy<sup>571</sup>. No other form of secrecy may be invoked before the Committee, with the exception of the professional secrecy of lawyers. The framework of control powers is completed by the possibility of access to and inspection of the offices of the services, which may only be refused in order not to interfere with ongoing operations.

In addition to these pervasive control powers, COPASIR acts as a counterweight to the executive, thanks to a series of reporting obligations on the part of the President of the Council<sup>572</sup>, which have always been a common approach, even in previous legislation. The

---

Segreto Di Stato: Una Coesistenza Problematica', *Giurisprudenza Costituzionale*, no. 5 (2015): 1719–37; Federico Gustavo Pizzetti, 'Il Più Recente Orientamento Della Corte Costituzionale Nel Caso Abu Omar: Novità Sul Segreto Di Stato?', *Processo Penale e Giustizia*, no. 6 (2014): 13; Roberto Prossomariti, 'Riflessioni Sul Segreto Di Stato a Partire Dal Caso Abu Omar: Quali Prospettive Dopo La Condanna Di Strasburgo?', *Costituzionalismo.It*, no. 1 (2016): 4.

<sup>569</sup> Article 39 of Law 124 of 2007 imposes a maximum overall limit of 30 years, taking into account any extensions of the restriction. Any extension must be justified by the President of the Council of Ministers and notified immediately to COPASIR.

<sup>570</sup> See Article 30 of Law 124 of 2007.

<sup>571</sup> Any need for security may be opposed by the addressee of the COPASIR request in order to avoid harming the security of the Republic or ongoing operations. If the Committee decides to insist on the request, it is submitted to the President of the Council, who must decide within 30 days whether the need for confidentiality exists. Confirmation can only be given in cases where state secrecy can be invoked. Confirmation could initially be overturned by COPASIR by a unanimous vote, but following a subsequent reform, a two-thirds majority is sufficient. See Article 31 of Law 124 of 2007, as amended by Article 6 of Law 133 of 2012. However, the doctrine points out that the reduction of the required majority may not be sufficient to promote effective knowledge of COPASIR. The actual effectiveness of the mechanism depends on the voting system envisaged for the deliberations. An open vote would make party discipline much easier, thus limiting COPASIR knowledge in the case of a solid government majority. Both the Chamber of Deputies' and the Senate's rules provide for a secret ballot for votes on persons. However, the vote could also refer to actions still attributed to unknown persons and fall under the system of open voting. An intervention to clarify the voting procedure would be desirable. See Gino Scaccia, "'Intelligence" e Segreto Di Stato Nella Legge n. 133 Del 2012', *Diritto e Società*, no. 3 (2012): 396–97.

<sup>572</sup> See Article 33 of Law 124 of 2007.



President is required to report every six months on the security policy and actions of the Services. In addition, all relevant information must be communicated in a timely manner. Examples include the authorisation of criminal conduct during an operation and the consequent imposition of state secrecy, or the expenditure and staffing status of the services. The Committee, in turn, submits an annual report to Parliament and reports to Parliament if it detects an irregularity<sup>573</sup>.

The Figure 20 summarises the above.

Figure 20 - Italian Intelligence after Law n. 124/2007

<sup>573</sup> See Article 34 of Law 124 of 2007.

#### IV.1.3 Reforms and amendments to Law 124 of 2007

The weakness of the Parliament was one of the reasons that led to the first corrective intervention in the new order of the services, which in just a few years had to face a rapidly changing domestic and international scenario. This was accompanied by the financial crisis, which had led to a rationalisation of intelligence expenditure and costs, as well as technological development<sup>575</sup>.

This last aspect could be grasped through the analyses periodically developed by the same bodies of the Intelligence System for the Security of the Republic. Already in 2009, the DIS had begun to devote space in its annual report to the new electronic communication technologies, which had become a dangerous tool for terrorist propaganda. The attention profile highlighted was that of the pervasiveness of this new dimension. Greater interconnectedness meant an ever-increasing danger due to the greater number of exploitable dependencies.

“Although the cyber threat concerns the intangible dimension of cyberspace, it is in fact capable of affecting a large number of interconnected sectors, including critical infrastructures. The gradual quantitative and qualitative increase in the number of actors involved plays a decisive role in demanding new attention from the information system”<sup>576</sup>.

Not only the executive, through the Services, but also Parliament was fully aware of the evolving scenario, which was moving towards the militarisation of what were beginning to look like real battlefields. “If, during the long interlude of the Cold War, technology was a factor of strategic superiority in the competition between the two superpowers, which were also committed to the militarisation of space and the development of computer networks that could serve their respective military strategies, today the emphasis is increasingly shifting to the virtualisation of international relations and thus, potentially, of conflicts”.<sup>577</sup> COPASIR had recognised the growing importance of the cyber-sphere to the lives of citizens and, echoing the words of US Secretary of State Hillary Clinton, had pointed out that an attack on one nation's computer network could be an attack on all of them<sup>578</sup>.

Both the executive and parliament were unanimous in stressing the need for a systemic reform to tackle the phenomenon, which at the time was the responsibility of a

---

that the report and its greater details are secret. Compare Article 11 of Law 801 of 1977 with Articles 33 and 39 of Law 124 of 2007.

<sup>575</sup> Scaccia, “‘Intelligence’ e Segreto Di Stato Nella Legge n. 133 Del 2012’, 585.

<sup>576</sup> My translation from Dipartimento Informazioni per la Sicurezza, ‘Relazione sulla politica dell’informazione per la sicurezza’ (Dipartimento Informazioni per la Sicurezza, 2009), 100, <https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2010/02/relazione-2009.pdf>. For a comment to the recent update of the regulatory framework see Melissa Ridolfi, ‘Servizi Di Informazione e Cybersicurezza’, *Giornale Di Diritto Amministrativo*, no. 2 (2023): 207–11.

<sup>577</sup> Comitato Parlamentare per la Sicurezza della Repubblica, ‘RELAZIONE sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall’utilizzo dello spazio cibernetico’, XXXIV (Comitato Parlamentare per la Sicurezza della Repubblica, 7 July 2010), 9, [https://www.parlamento.it/documenti/repository/commissioni/bicamerale/COMITATO%20SICUREZZA/Doc\\_XXIV\\_n\\_4.pdf](https://www.parlamento.it/documenti/repository/commissioni/bicamerale/COMITATO%20SICUREZZA/Doc_XXIV_n_4.pdf).

<sup>578</sup> The new digital dimension leads to a reversal of the military logic typical of traditional warfare, due to the anonymity that the Net allows. The balances of deterrence that characterised the Cold War no longer exist in the face of the possibility of attacking and potentially going unpunished. The new mechanisms were analysed at the time by Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, 1st ed. (New York: HarperCollins, 2010).

heterogeneous range of actors at national level<sup>579</sup>.

This included the intelligence Services<sup>580</sup>, which were informally assigned tasks in the prevention of cyber threats in the absence of a formal mandate. The exceptional and sporadic nature of the actions taken by the institutions, which had previously served “individual organisational gaps”<sup>581</sup>, was recognised.

There was an urgent need to modernise the existing arrangements in order to achieve coordinated and unified planning at the level of the political summit, which should have been represented by the President of the Council of Ministers, in line with the role already exercised within the Information System. The reorganisation should have provided an overall vision that would have responded in an integrated manner to the protection needs of critical infrastructure and the need for public-private coordination. More than a decade ago, COPASIR spoke of “preparing an action plan that defines the scope of Italian cybersecurity and defines the roles and responsibilities of all the actors responsible for national cybersecurity”<sup>582</sup>. On this point, the recommendation to the government was explicit, because “the absence of a strategic review of the national security perimeter implied, directly and indirectly, a sub-optimal investment in terms of policy and protection of national interests”<sup>583</sup>.

Faced with all these problems, the legislator intervened to amend Law 124 of 2007 and bring the system up to date. The competence to intervene in cyberspace was thus enshrined in Law 133 of 2012. The High Security Intelligence Directive expressly provides for the power to issue the necessary coordination directives after consulting the Interministerial Committee for the Security of the Republic. Coordination can also be aimed at strengthening national cyber protection and cyber security<sup>584</sup>. This formalised the link between cyber security and the intelligence services, whose activities would be described in a specific document attached to the annual report to Parliament<sup>585</sup>.

However, the intervention had not only concerned cyber security, but had also worked towards a comprehensive strengthening of the Republic's security information system.

In particular, a process of autonomisation of the functions of intelligence governance can

---

<sup>579</sup> The main activity in Italy was the fight against cybercrime through the use of specialised police forces. Article 7-bis of Legislative Decree No. 144 of 27 July 2005 entrusted the Postal and Communications Police with the task of ensuring the cyber protection of critical information infrastructures of national interest, identified by decree of the Minister of the Interior. The Postal and Communications Police were then joined by the National Centre for the Protection of Critical Information Infrastructures against Computer Crime (in Italian *Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche* or CNAIPIC), which was formally established by decree of the Chief of Police on 7 August 2008, in accordance with the decree of the Minister of the Interior of 9 January 2008. For further information, please consult Comitato Parlamentare per la Sicurezza della Repubblica, ‘RELAZIONE sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall’utilizzo dello spazio cibernetico’, 36–47.

<sup>580</sup> The INFOSEC Division of the AISE, the Telematics Counter-Intelligence Division of the AISI and the Central Office for Secrecy (UCSE) of the DIS should be mentioned.

<sup>581</sup> Comitato Parlamentare per la Sicurezza della Repubblica, ‘RELAZIONE sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall’utilizzo dello spazio cibernetico’, 49.

<sup>582</sup> Comitato Parlamentare per la Sicurezza della Repubblica, 50.

<sup>583</sup> Comitato Parlamentare per la Sicurezza della Repubblica, 52.

<sup>584</sup> See article 1, paragraph 3-bis, as introduced by article 1 of law 133 of 2012.

<sup>585</sup> See article 38, paragraph 1-bis, as introduced by article 9 of law 133 of 2012.

be observed<sup>586</sup>. The introduction of restrictions on the possibility of delegating the non-exclusive powers of the President of the Council of Ministers prevented the delegated authority from exercising other governmental functions. The importance of the role and the delicacy of the issues concerning the Services had led the legislator to opt for complete dedication to the matter.

On the parliamentary side, however, corrective measures were taken to extend and deepen COPASIR's powers of control.

This had become necessary because of the heterogeneous nature of the cooperation between the departments, which can draw on the activities of structures outside the information system but which are closely linked to it. The Committee's control came up against a restrictive formulation of its prerogatives, which ignored this complexity of relations. Despite the fact that all bodies outside the intelligence system were prohibited from carrying out the typical functions of the Services, the powers of control were directed only at those belonging to the system. As a result, COPASIR could have monitored the excesses of the intelligence system, but could not have monitored entities outside the system, no matter how closely they operated. The change in the scope of the control powers removed this contradiction<sup>587</sup>.

The widening of the scope of the Committee's control also meant a strengthening of its powers of intervention. Whereas it had previously only been able to inform the President of the Council of the infringements it had detected and to report to the Presidents of the Chambers, it now had the power to propose to the President that internal investigations be carried out<sup>588</sup>. This does not entail any obligation on the part of the executive, but if the investigation is carried out, all final reports must be sent to COPASIR.

To conclude this summary of the main interventions of the reform, it should be recalled that the legislature's intervention came after a series of relevant rulings by the Constitutional Court on the subject of substantive control over state secrecy<sup>589</sup>. On the basis of the

---

<sup>586</sup> Scaccia, "Intelligence" e Segreto Di Stato Nella Legge n. 133 Del 2012', 587.

<sup>587</sup> See Article 30, paragraph 2-bis of Law 124 of 2007, as introduced by Article 5 of Law 133 of 2012.

<sup>588</sup> See Article 34 of Law 124 of 2007, as amended by Article 8 of Law 133 of 2012.

<sup>589</sup> The reference is to the decisions of the Constitutional Court 106 of 2009 and 40 of 2012. In these rulings, the Court confirmed that the parliamentary forum is the most appropriate for the control of the disclosure of state secrets. As a result, the Court had set certain limits to its possibility of control, so as not to express a political review. By briefly summarising the steps that characterised the development of the case law, it is possible to recall the three characteristic judgments on the subject. All of them are based on an incidental judgment issued by the criminal court on the basis of the affixing of the state secret. Judgement 86 of 1977, which emphasised the scope of the political discretion underlying the activity of secrecy, justified removing it from the control of the judicial authority and subjecting it only to the political control of Parliament. Judgment 106 of 2009 had limited the Court's intervention in the conflict to a mere assessment of the "existence or non-existence of the conditions for secrecy". In other words, the Court had declared that it was prevented from acting on the basis of the principles of legality and proportionality, because otherwise its judgment would have interfered with the substance of the reasons. It should be stressed, however, that this approach could be countered by the fact that a judgement on a political act is not in itself a judgement on its merits, as the doctrine has already reiterated. See among others Adele Anzon Demmig, 'Il Segreto Di Stato Ancora Una Volta Tra Presidente Del Consiglio, Autorità Giudiziaria e Corte Costituzionale', *Giurisprudenza Costituzionale*, no. 2 (2009): 1020–33. Judgment 40 of 2012 continues in this direction, further hardening the position. The Court responds to the criminal court by stating that the verification of the existence of evidence against the accused within the sealed facts would constitute an "incorrect overlap between the object of the conflict and the object of the criminal trial". The answer is clearly aimed at reducing the Court's scope of action, whereas the verification of the abuse of power

jurisprudential confirmation of the need for political control to balance the imposition of secrecy, the legislature intervened to correct the malfunctioning that had occurred since the first implementation of the reform in 2007.

The President of the Council is required to inform COPASIR of any confirmation of secrecy, stating the main reasons for authorising its monitoring activities<sup>590</sup>. Unfortunately, the practice of interpretation that had become customary had led the government to provide meagre documentary elements, “insufficient to enable a truly penetrating political control to be exercised in practice”<sup>591</sup>. In other words, the essentiality of the reasons had not been assessed in relation to parliamentary control, but as a general criterion relating to documentary data.

The reform responded to this need by “bringing the function of protecting state secrets back into line with the postulates of the parliamentary form of government outlined in the Constitution”<sup>592</sup>. Although the expression “essential reasons” is retained, the power of the President of the COPASIR to summon the President of the Council to a secret meeting in order to obtain from him the appropriate information framework is introduced. The use of the word “expose” seems to imply only an oral treatment of the matter<sup>593</sup>.

This underlines the responsibility of the President, who must appear in person before the committee, albeit in secret. The possibility of being summoned can also be seen as a deterrent against the excessive use of state secrecy, which must always remain exceptional in relation to the general principle of transparency of the administration's actions.

Despite this undoubted improvement in the Committee's monitoring capacity, we are still a long way from an efficient system. Now that various contingencies have led to the confirmation of a strong government majority, the fact that the committee can only report to Parliament is completely inadequate. With a parliament of the same political colour as the

---

has always been one of its physiological attributions. This would not mean going into the merits of the decision, but checking whether the government has exercised its prerogatives properly. In short, the Court should be entitled to verify whether secrecy is essential to protect the integrity of the Republic, the independence of the State and its military defence. The preponderance of secrecy should be affirmed in the physiological balance of constitutional values applied in the concrete case. Reference is made to Adele Anzon Demmig, ‘La Corte Abbandona Definitivamente All’esclusivo Dominio Dell’autorità Politica La Gestione Del Segreto Di Stato Nel Processo Penale’, *Giurisprudenza Costituzionale*, no. 1 (2012): 534–37. The result of the balance drawn by the Constitutional Court is that it plays only a servant's role in relation to Parliament. Its task is to verify that the latter has all the necessary elements to assess the actions of the executive, i.e. that the information provided by the President of the Council of Ministers is sufficiently detailed. On the one hand, the Court verifies the conformity of the secret activity with the constitutional parameters for its non-discretionary aspects. On the other hand, Parliament examines the political value of the secrecy. Reference is made to Scaccia, “‘Intelligence’ e Segreto Di Stato Nella Legge n. 133 Del 2012’, 595.

<sup>590</sup> This was also what emerged from the Constitutional Court's ruling 86 of 1977. Please refer to the operative part.

<sup>591</sup> Scaccia, “‘Intelligence’ e Segreto Di Stato Nella Legge n. 133 Del 2012’, 591.

<sup>592</sup> Scaccia, 591.

<sup>593</sup> See Articles 40 and 41 of Law 124 of 2007, as amended by Articles 10 and 11 of Law 133 of 2012. An earlier draft law had proposed an even stricter mechanism, obliging the President of the Council to provide a full picture of the situation, but only to the President and Vice-President of COPASIR. In this way, the opposition and the political majority would have been equally informed of the decision. This proposal was rejected because it would have created dangerous asymmetries of information within the committee. In addition, it would have led to an excess of information that was disproportionate to the purpose of parliamentary scrutiny. It is not necessary for COPASIR to know all the details of the secrecy, but it is sufficient for it to be able to assess the merits.

government, it would be very difficult to get any concrete action. A possible corrective could be to oblige the parliamentary chambers to deliberate by secret ballot.

At the same time, the rules of operation of COPASIR should be revised to make it easier to activate the conflict of competences before the Constitutional Court<sup>594</sup>.

#### IV.1.4 Il D.P.C.M. 24 January 2013 (Monti's decree)

The National Cybersecurity System (in Italian, Sistema Nazionale di Sicurezza Cibernetica or SNSC) had been outlined on this regulatory framework, which represented an attempt to unify cybersecurity efforts. Cybersecurity had begun to sprout from the institutional body of the Security Information System of the Republic.

To be clear, Italy was not lacking in the definition of procedures and bodies to deal with crisis situations, but these were still geared towards responding to traditional types of situations<sup>595</sup>.

Faced with international pressure, both from NATO and from other EU countries, the legislature had recognised the need to intervene. On 23 May 2012, a motion in the Senate compelled the government to move in this direction<sup>596</sup>.

The increasing frequency and severity of cyber-attacks made it imperative to complete the protection systems, which were at that time rather unevenly developed. Priorities for action needed to be defined and the most appropriate roles assigned in order to stimulate multilateral cooperation. In particular, there was a specific call for the establishment of an inter-ministerial committee within the President of the Council's Office with the task of strategic coordination in the field of cyber security. This should have also play a political role in setting policy priorities through binding directives and defining a national strategy.

All these needs were addressed by the aforementioned Monti Decree<sup>597</sup>, which was a first attempt to unify the matter. In this respect, it can be seen as a kind of forerunner of the current national cyber security perimeter. Certainly, both the scale and the context were different, but this law marked the beginning of a path of gradual and progressive

---

<sup>594</sup> Some propose the introduction of a voting mechanism whereby a proposal is accepted if it is not rejected by a majority of votes. Scaccia, "Intelligence" e Segreto Di Stato Nella Legge n. 133 Del 2012', 597–98. The issue of majorities, far from being secondary, has always gone hand in hand with heterogeneous management. Law 124 of 2007 provides for different majorities depending on the case. For example, while a precise majority is required for the overcoming of secrecy when COPASIR has ordered investigations into the conformity of the conduct of members of the security intelligence services with their institutional duties, there is no indication for the overcoming of secrecy against the judicial authority. Similarly, there is no explicit majority for cases in which the committee decides to report to the Chambers once a breach has been established. In conclusion, "the combined provisions of the various provisions of the law therefore deny the powers (and competences) of the Committee with regard to the State secret according to different cases and are not subject to a single general rule". "The very fact that there is no provision for a majority increases the risk of internal conflicts within the Committee, based on partisan motives rather than on the unitary interest of defending the Republic". See Marco Franchini, 'Alcune Considerazioni Sulle Nuove Competenze Del Comitato Parlamentare per La Sicurezza Della Repubblica', *Rivista AIC*, no. 1 (2014): 10.

<sup>595</sup> The government rationalised the previous rules partially by D.P.C.M. of 5 May 2010 and partially by D.P.C.M. of 1 October 2012.

<sup>596</sup> Senato della Repubblica, 'Mozioni 23 maggio 2012, n. 1-00405 e n. 1-00491', 23 May 2012, [https://www.sicurezzacibernetica.it/db/\[2012\]%20Mozioni%2023%20maggio%202012,%20n.%201-00405%20e%20n.%201-00491%20-%20Mozioni%20sulla%20sicurezza%20da%20minaccia%20cibernetica.pdf](https://www.sicurezzacibernetica.it/db/[2012]%20Mozioni%2023%20maggio%202012,%20n.%201-00405%20e%20n.%201-00491%20-%20Mozioni%20sulla%20sicurezza%20da%20minaccia%20cibernetica.pdf).

<sup>597</sup> 'DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 24 gennaio 2013', 24 January 2013, <https://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg>. For one of the few comments, please see Franchina, 'Le Infrastrutture Critiche e La Protezione Cibernetica Nazionale', 201.

rationalisation of roles, tools and procedures.

A multi-level system for cyber security was outlined. The first level is the political level, which is responsible for setting functional objectives for national cyber protection and cyber security. In order to pursue these objectives, a support level was added with the task of interconnecting all relevant public administrations. An important component in the integration of the various bodies involved is the use of security intelligence, which is a fundamental source for identifying threats and strengthening security measures accordingly. The last level is specifically dedicated to crisis management through the coordination of response activities.

The aim of this structure was to implement the new "institutional architecture entrusted with the protection of national security with regard to material and immaterial critical infrastructures, with particular reference to national cyber protection and cyber security"<sup>598</sup>. The definition of roles and procedures was preparatory to a timely response, to be combined in full respect of the functions already attributed to each actor. In this sense, the decree does not replace or conflict with existing legislation, but acts as a connecting interface between new and existing actors. Its great virtue lies in its ability to harness and integrate existing competences for an orchestration aimed at cybersecurity. As mentioned above, much of the architecture is based on the balances established by Law 124 of 2007.

The President of the Council of Ministers retains a central role, with the task of adopting and updating policy documents. On the one hand, the national strategic framework for the security of cyberspace, which includes the identification of threats and vulnerabilities, but above all the roles, tasks and procedures for improving security. On the other hand, the national cyber protection plan, which contains the objectives to be achieved and the lines of action to implement the strategic framework. In general, the President retains the power of direction, assisted by the CISR, which drafts and proposes both the strategic framework and the national plan for adoption<sup>599</sup>.

The Interministerial Committee plays both an advisory role, including in the updating of the system, and an executive role with regard to the Prime Minister's directives. It can give its opinion on the President's acts, but above all it is responsible for their implementation. To this end, it monitors and supervises the implementation of the National Cyberspace Security Plan. The development of general guidelines and objectives for national cyber security is not secondary. Above all, the committee plays a key role in advising and making proposals to the President in crisis situations<sup>600</sup>.

Since the performance of all these activities requires a high degree of specialisation, the system provides the political bodies with appropriate support systems. These are based on the organisational structures of the DIS. On the one hand, the so-called Collegial Coordinating Body (in Italian *organismo collegiale di coordinamento*), which deals with the organisation and functioning of the DIS, is explicitly identified as a support body<sup>601</sup>. Chaired by the Director General of the DIS, it becomes an important point of contact for other bodies through the

---

<sup>598</sup> See article 1 of the D.P.C.M. under examination.

<sup>599</sup> See article 3 of the D.P.C.M. under examination.

<sup>600</sup> See article 4 of the D.P.C.M. under examination.

<sup>601</sup> This body was set up on the basis of article 4, paragraph 5, of the D.P.C.M. of 26 October 2012 ("Regulation and organisation of the Ministry of Security and Intelligence"). In the jargon, it is also known as the "technical CISR", a definition introduced after the reform of the D.P.C.M. of 17 February 2017.

participation of the Military Adviser, whose office is located within the Presidency of the Council of Ministers. The Support Body mainly performs a preparatory and preliminary function with regard to the meetings and actions of the CISR. It also carries out the material activities of verifying the proper implementation of the National Plan. If the committee is formally charged with the task of verifying the implementation of the plan, the preparatory activities for this purpose are carried out by the support body. It is this body that provides the necessary guidance for identifying threats, vulnerabilities and their mitigation through good practice and security measures<sup>602</sup>.

On the other hand, the structures dedicated to the training of intelligence personnel are also involved in the support activities. A scientific committee is set up within the training school, bringing together representatives from research, the administration and the private sector. Although the committee does not contribute directly to the CISR, it does contribute indirectly by supporting the collegial coordination body, which can benefit from its scientific background<sup>603</sup>.

In general, the intelligence system contributes to the country's cyber security through its capacity to collect and process information, always in accordance with the President of the Council's guidelines. The agencies can benefit from privileged sources through special agreements with public administrations. The intelligence research activity is coordinated by the Director General of the DIS, who is able to formulate analyses, evaluations and forecasts for increasing national cyber security through the information available<sup>604</sup>.

This level of support, which largely relies on existing competences and bodies within the intelligence system for the security of the Republic, is complemented by new bodies aimed at better coordinating cybersecurity crises. As already mentioned, there was no lack of instruments to deal with traditional crises, but they had to be adequately supplemented in view of the specific expertise required to deal with the new threats. The reference is to the Cybernetic Security Unit (in Italian *Nucleo per la sicurezza cibernetica*), set up in the office of the Military Adviser, who chairs it. It brings together representatives of all the administrations involved in national cybersecurity, with the possibility of expansion depending on the subject, and therefore plays a fundamental coordinating role in the management of cyber crises. It is also the appropriate forum for the preparation of operational procedures for crisis response by all actors involved and for the exchange of relevant information or alerts. All information regarding security breaches or attempted breaches must flow into the Unit from the Ministry of Economic Development, which previously hosted the national CERT, the Ministry of Defence, the Ministry of the Interior and the police forces. A permanent alert unit will be set up at the Cybernetic Security Unit to collect and issue alerts to administrations and private operators.

The central role of internal coordination is matched by a liaison role with the international organisations of which Italy is a member: the UN, NATO and the EU<sup>605</sup>.

Despite its key role, the actual crisis management was, at least initially, entrusted to another body. If the Cybernetic Security Unit judged that the scale of the security event was such as to require interministerial coordination, it could declare a cyber crisis situation and

---

<sup>602</sup> See article 5 of the D.P.C.M. under examination.

<sup>603</sup> See article 6 of the D.P.C.M. under examination.

<sup>604</sup> See article 7 of the D.P.C.M. under examination.

<sup>605</sup> See articles 8 and 9 of the D.P.C.M. under examination.



activate the Interministerial Cyber Crisis Table (in Italian *Tavolo interministeriale di crisi cibernetica*). The latter was established in the Nucleo interministeriale situazione e pianificazione (in Italian *Nucleo interministeriale situazione e pianificazione* or NISP), a body already existing in the national crisis management organisation. The D.P.C.M. under review extends its competences to include cyber crises<sup>606</sup>.

The objective was always to ensure the coordinated exercise of crisis response, management and recovery activities by entities belonging to different administrations. To this end, it could rely on the technical support of the national CERT.

Unlike the Cybernetic Security Unit, the Table had an operational role during the crisis, keeping the President of the Council of Ministers informed. The information gathered was processed into reports to be distributed to the public and private actors concerned. At the same time, it ensured ministerial and international coordination with foreign counterparts and international organisations<sup>607</sup>.

Last but not least, the system outlined by the Prime Ministerial Decree did not neglect the contribution of private operators to national IT security. The obligations to notify incidents and to implement technical and organisational security measures, laid down in Article 16-bis of Legislative Decree 259 of 2003 for operators of public communications networks or publicly accessible electronic communications services, had been extended to all operators of critical infrastructures of national and European importance. The vital importance of these services had led to the introduction of an obligation to provide information to security intelligence services, allowing them access to databases of interest<sup>608</sup>.

The following figure condenses the relationships and dependencies just described, grafting them onto the structure of the former Republic Security Intelligence System.

---

<sup>606</sup> To this end, the composition was expanded to include a representative of the Ministry of Economic Development and AgID. It should be noted that the table, normally chaired by the Undersecretary of the Presidency of the Council of Ministers, was instead chaired by the Military Counsellor in the event of a cyber crisis. Compare article 5 of the D.P.C.M. of 5 May 2010 with article 10 of the D.P.C.M. of 24 January 2013.

<sup>607</sup> See article 10 of the D.P.C.M. under examination.

<sup>608</sup> See article 11 of the D.P.C.M. under examination.

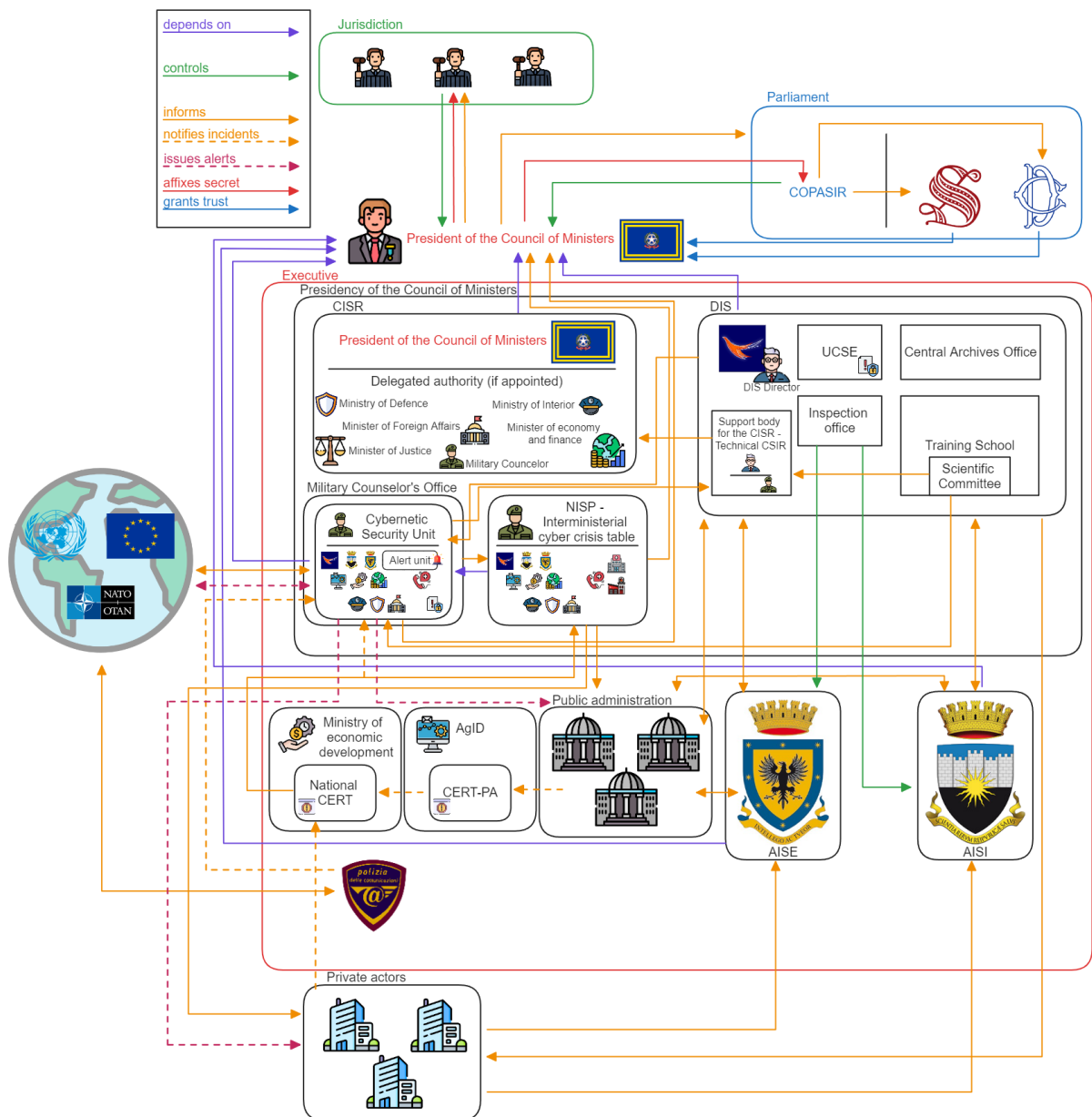


Figure 21 - The Italian Cybersecurity Framework (D.P.C.M. Monti)

#### IV.1.5 Il D.P.C.M. 17 February 2017 (Gentiloni's decree)

This direction was confirmed by subsequent legislative interventions, which extended the competences and economic availability available.

Article 7-bis paragraph 5 of Decree-Law 174 of 30 October 2015 had intervened by assigning to the Inter-Ministerial Committee for the Security of the Republic (CISR) the tasks of consultation, advice and proposal to assist the Prime Minister in the event of crisis situations affecting national security.

In addition, the final adoption of the first NIS Directive the following year confronted the national legislator with the need to update the institutional architecture in view of the transposition of European legislation. The system needed to be brought back into line in terms of responsibilities for crisis management.

While awaiting the transposition of the directive, the then Premier Gentiloni intervened

with a D.P.C.M. to meet this need for renewal<sup>609</sup>.

On the basis of the imprint dictated by Parliament through the previous interventions, one can see the clear separation of traditional crisis management mechanisms from those dedicated to cyber crisis management. The latter acquire an autonomous dignity due to their specific nature. At the same time, the NIS terminologies of essential service operators and digital service providers are adopted from the outset.

The role of the President of the Council of Ministers is strengthened with the express provision that, after hearing the opinion of the CISR, which he may convene with the precise function of advising, proposing and deliberating in the event of a national security crisis, he will define measures to deal with the crisis<sup>610</sup>. In this way, in the event of a crisis, the CISR becomes a participant in the President's decisions<sup>611</sup>.

There is also a reorganisation of the supporting bodies. On the one hand, the training school and its scientific committee are removed from the security architecture. On the other hand, the CISR support body is renamed the Technical CISR, although it retains the same functions. The only major change is in its composition, with the removal of the military adviser, in line with the reorganisation of the bodies dealing with crisis management and response<sup>612</sup>.

On the other hand, the role of the General Director of the DIS is strengthened as a reference point for the coordination of the information research activities of the two intelligence services. It is up to him to define the lines of action to increase the security level of systems and networks, using the appropriate technological support. To this end, the Director can set up the appropriate organisational modules and make use of expertise within the public administration and private bodies<sup>613</sup>.

As mentioned above, the most significant changes concern the mechanisms for managing cyber crisis situations. Whereas previously there was a division of tasks between two separate bodies, the Cyber Security Unit and the Interministerial Cyber Crisis Table, all these functions have been merged into the Unit<sup>614</sup>. The latter is now the sole steering body following its relocation within the DIS. As a result, it is no longer chaired by the military adviser, who remains a member, but by one of the deputy directors of the DIS. The direct link with the President of the Council is lost, as information is channelled through the Director-General of the DIS, who must be kept constantly informed of crises. Technical support, previously limited to the national CERT, is extended so that the entire network of CERTs can provide technical

---

<sup>609</sup> 'DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 17 febbraio 2017', 02 2017, <https://www.gazzettaufficiale.it/eli/id/2017/04/13/17A02655/sg>. For a commentary on precisely this period of transition, see Maria Salamone and Di Luca Vincenzo, 'La Disciplina Del "Cyberspace" Alla Luce Della Direttiva Europea Sulla Sicurezza Delle Reti e Dell'informazione: Contesto Normativo Nazionale Di Riferimento, Ruolo Dell'"intelligence" e Prospettive "de lure Condendo"', *Federalismi.It*, no. 23 (2017): 28–33.

<sup>610</sup> See article 3 of the D.P.C.M. under examination.

<sup>611</sup> See article 4 of the D.P.C.M. under examination.

<sup>612</sup> See article 5 of the D.P.C.M. under examination.

<sup>613</sup> See articles 6 and 7 of the D.P.C.M. under examination.

<sup>614</sup> After the Unit declares a crisis situation requiring inter-ministerial coordination, its composition is integrated in a manner similar to that of the Inter-Ministerial Cyber Crisis Table. It includes a representative of the Ministry of Health, the Ministry of Infrastructure and Transport, the Department of Fire, Public Rescue and Civil Defence and the Office of the Military Counsellor to the President of the Council of Ministers.

support to the Unit<sup>615</sup>.

Although the obligations of private actors were not modified, in line with the transposition requirements of the NIS Directive, it is worth mentioning the establishment of the National Evaluation and Certification Centre (in Italian *Centro di Valutazione e Certificazione Nazionale* or CVCN) at the Ministry of Economic Development, which today constitutes a key component of the security Perimeter<sup>616</sup>. The aim of the Centre was to make its services for verifying the security conditions and vulnerabilities of products available to all stakeholders.

Summarising the main interventions, a twofold feature immediately emerges. The powers of the DIS and the CISR have been strengthened, while at the same time the chain of command has been simplified by introducing more streamlined coordination procedures. The exchange of information is managed more efficiently in order to permeate the entire cybersecurity system.

This simplification is illustrated in Figure 22.

---

<sup>615</sup> See articles 8, 9, and 10 of the D.P.C.M. under examination.

<sup>616</sup> See article 11 of the D.P.C.M. under examination. As will be seen in the following paragraph, the actual activation of the CVCN required further action, but its establishment was a key moment for the Italian security landscape.

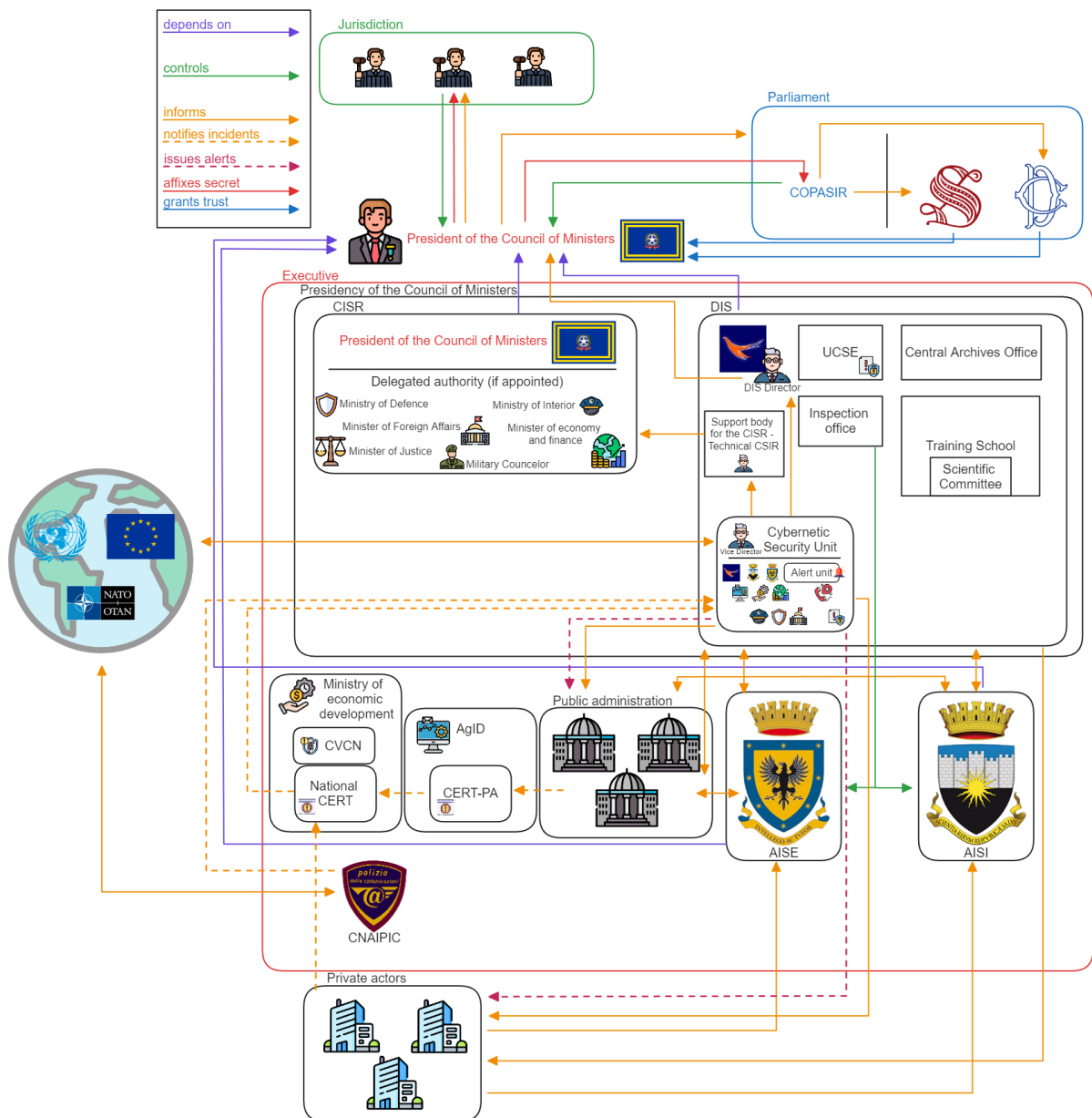


Figure 22 - The Italian Cybersecurity Framework after D.P.C.M. Gentiloni

The disappearance of the many existing intermediary relationships for the exchange of information brought the role of the DIS to the spotlight, initiating the process of orchestrating Italian cybersecurity that would later culminate in the creation of the National Cybersecurity Agency (in Italian *Agenzia per la cybersecurity nazionale* or ACN). It was precisely “the lack of centralised and unified governance that was the mother of all problems for Italian cybersecurity”<sup>617</sup>. The establishment of a system centred on the DIS had created the conditions for real support to the President of the Council of Ministers and an effective link between the CISR, the administration and the private sector.

This centrality had been maintained and had also guided the implementation of the NIS Directive, which had been transposed by Legislative Decree 65 of 18 May 2018.

<sup>617</sup> Salamone and Vincenzo, ‘La Disciplina Del “Cyberspace” Alla Luce Della Direttiva Europea Sulla Sicurezza Delle Reti e Dell’informazione’, 30.

In a manner fully consistent with the security architecture prepared and described here, the DIS was identified as the single point of contact for relations with counterparts in other European countries<sup>618</sup>.

From its key role as a Service Coordination Point, it had gradually taken on other connotations after the replacement of CESIS. From the cyber intelligence function, a cyber resilience function, previously sporadically assigned to heterogeneous actors, began to emerge and become autonomous. If the electronic communications sector had been the first test-bed for the introduction of obligations to report security incidents and to implement adequate security measures, this was followed by the data protection sector and then a more systematic management with the NIS system.

This had greatly simplified the flow of information by merging the national CERT and the CERT-PA into a single Computer Security Incident Response Team (CSIRT) at the Presidency of the Council of the Ministers<sup>619</sup>. All incident reports were then collected and distributed to both the Technical Liaison Committee, representing the national NIS authorities, and to all those bodies to which individual CERTs had previously contributed.

Figure 23 shows the end point of the national security architecture after the transposition of the NIS Directive.

---

<sup>618</sup> For a more detailed description of European legislation, please refer to paragraph III.

<sup>619</sup> See article 8 of Legislative Decree 65 of 2018. The CSIRT was officially established by the Prime Ministerial Decree of 8 August 2019, which established its operating mechanism.



of key European laws, from the G.D.P.R. to the Cybersecurity Law<sup>620</sup>, had confronted the Italian legal system with the need for rapid adaptation.

Although the EU reforms had been announced for some time, as part of a systemic framework, the first definition of which can be found in the EU's first cybersecurity strategy<sup>621</sup>, their driving force on individual national legal systems should not be overlooked. As is well known, internal adaptation is not limited to the simple transposition of directives in a totally reactive manner but must seek to anticipate system-wide impacts and inconsistencies. As a result, further contextual changes are often necessary to pursue the European direction. This is all the more true when it comes to issues that are closely linked to the interests of nation states, such as cybersecurity.

Faced with these needs, Italy did not start from scratch, given the initial developments following the so-called Monti Prime Ministerial Decree. As we have seen, this had led to the elaboration of the National Strategic Framework for Cyberspace Security and the first National Plan for Cyber Protection and Cyber Security.

Later, in preparation for the transposition of the first NIS Directive, the Prime Minister had again intervened in the security architecture for a first adaptation of the system of bodies and powers. The so-called Gentiloni decree had favoured a general simplification in order to meet the deadline for the subsequent transposition decree, which was not adopted until the following year.

Legislative Decree 65 of 2018 had been based on this, continuing this partial work of adaptation to the European order. As expected, the changed legislative scenario had affected the architecture to the point that it could be considered outdated.

However, this was not just a question of legislation. Although the Union had taken a leading role in the field of cyber security, in many respects it was still unable to keep up with the increasingly rapid pace of technological development.

To avoid repeating in full the observations already expressed in the introductory chapter on European policies, it is sufficient to refer to the next generation of communication networks (5G). In the age of digital convergence, they represent a vast and pervasive attack surface. The variety of services to which they can provide access highlights the seriousness of the consequences of compromising these infrastructures. Not only would there certainly be a cross-sectoral impact, but “any significant vulnerabilities and/or cybersecurity incidents concerning 5G networks happening in one Member State would affect the Union as a whole”<sup>622</sup>. Certainly, the European Commission was well aware of the strategic value of the cybersecurity of 5G networks when it adopted its recommendation on the subject and launched a risk assessment process of the entire sector at European level<sup>623</sup>. The world had changed since the first cybersecurity strategy was drafted, and the continuation of Europe's digitalisation had to take this into account.

Although only in the national context, since 2018 Clusit has tried to highlight the changing times in its annual cybersecurity report. Using a variety of metaphors, the association

---

<sup>620</sup> Please refer to chapter III for more details.

<sup>621</sup> Please refer to paragraph II.3.2 for more details.

<sup>622</sup> European Commission, ‘OJ L 88, 29.3.2019, p. 42–47’, 1.

<sup>623</sup> Member States were invited to update their security requirements and to assist ENISA in preparing the risk assessment. At the same time, the NIS Co-operation Group was requested to identify best practices adopted at national level in order to enable all states to adopt the most appropriate risk mitigation measures.



photographed the ever-worsening threat scenario. First, it compared the situation of chronic insecurity to a "quantum leap in the level of global cybersecurity"<sup>624</sup> and then declared that we are now "two minutes to midnight", echoing the image of the "Doomsday Clock"<sup>625</sup>.

Macabre as it is, the comparison supports the view that "the trends we are observing cannot continue much longer without causing some kind of discontinuity, some kind of rupture (even if we have no way of knowing how this will happen), and that the stress the system can still bear is limited"<sup>626</sup>. We are not just talking about a simple quantitative increase in attacks, but a significant increase in their average severity. As a result, although the threat categories are always the same, there is a big difference in the potential impact of the same category over time. An attack that was considered exceptional yesterday quickly becomes the new normal, while new exceptional threats emerge<sup>627</sup>.

---

<sup>624</sup> See the Clusit 2018 report covering 2017, here Associazione Italiana per la Sicurezza Informatica, 'Rapporto Clusit 2018 sulla sicurezza ICT in Italia' (Clusit, September 2018), 10, [https://clusit.it/wp-content/uploads/download/Rapporto\\_Clusit\\_2018\\_aggiornamento\\_settembre.pdf](https://clusit.it/wp-content/uploads/download/Rapporto_Clusit_2018_aggiornamento_settembre.pdf).

<sup>625</sup> Conceived in 1947 by scientists at the University of Chicago's Bulletin of the Atomic Scientists, this special clock marks the time remaining until the end of the world due to an impending nuclear apocalypse. If midnight is used to represent the X-hour, being 'two minutes away' means being close to the end. See Clusit's 2019 report on 2018 Associazione Italiana per la Sicurezza Informatica, 'Rapporto Clusit 2019 sulla sicurezza ICT in Italia' (Clusit, September 2019), 12, [https://clusit.it/wp-content/uploads/download/Rapporto\\_Clusit\\_2019\\_aggiornamento\\_settembre.pdf](https://clusit.it/wp-content/uploads/download/Rapporto_Clusit_2019_aggiornamento_settembre.pdf).

<sup>626</sup> My translation from Associazione Italiana per la Sicurezza Informatica, 12.

<sup>627</sup> If until 2017 organised crime was considered the new trend, in less than a year this category has become representative of the majority of attacks. At the same time, the terms cyberwar or cyberespionage have entered the lexicon, a symptom of the existence of far worse threats. As early as 2012, NATO had begun to define cyberspace as a "non-domain" in which to conduct its operations, as it is closely linked to the protection of states' national security. While there are several technical definitions that can be agreed upon, the distinguishing feature is that global actors can also develop their own policies within it. For definitions see Alexander Klimburg and NATO Cooperative Cyber Defence Centre of Excellence, *National Cyber Security Framework Manual* (Tallinn, Estonia: NATO Cooperative Cyber Defense Center of Excellence, 2012), <http://ccdcoe.org/369.html>.

This includes behaviour that often takes the form of direct attacks on services and infrastructure with the aim of stealing information or disrupting their functioning. Already in 2016, the European Union had recognised the growing importance of cyber threats and started to strengthen its Common Security and Defence Policy (CSDP) to enforce responsible state behaviour also in cyberspace. Confirming this, the Union's Strategic Compass also highlighted how fragile international multilateralism is currently threatened by a complex threat scenario. Cyberspace is now a strategic competitive domain "where state and non-state actors use hybrid strategies, cyber-attacks, disinformation campaigns, direct interference in elections and political processes" [my translation]. See Council of the European Union, 'Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign and Security Policy', 22–23; Council of the European Union, 'A Strategic Compass for Security and Defence - For a European Union That Protects Its Citizens, Values and Interests and Contributes to International Peace and Security', 21 March 2022, 11–12, 7371/22, <https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf>.

The general management of relations in the digital domain therefore requires knowledge of a heterogeneous set of problems that are not limited to aspects of cybersecurity. Although the latter is recognised as one of the main risks to the global order by the recent World Economic Forum report, which highlights its short- and medium-term impact, it must be placed in a broader context, in which other instruments of aggression are also present. Compare 'The Global Risks Report 2023', Insight Report (World Economic Forum, January 2023), 6–11. We often speak of hybrid threats, which combine elements of traditional warfare (such as kinetic attacks) with cyber-attacks, disinformation campaigns and other non-kinetic tactics. Information manipulation has been the subject of increasing interest in recent years, such as the Russian interference in the 2016 US presidential election campaign, the false information spread during the COVID-19 pandemic, or the war propaganda that characterises the current conflict in Ukraine. Disinformation has found a place in the EU's plans to ensure global

Following this crescendo, the 2020 report then emblematically christened 2019 after the Pillars of Hercules as the unexplored land, marked on nautical charts by the Latin phrase 'Hic Sunt Leones'<sup>628</sup>. It was in this context that the Italian legislator intervened to create the National Perimeter, ideally responding to the call for more regulation from cybersecurity experts.

The Decree-Law was justified precisely by the extraordinary necessity and urgency of the "ongoing construction of important and strategic technological infrastructures, also in the light of recent attacks on the networks of European countries". It was therefore essential to have "a system of bodies, procedures and measures for the effective technical evaluation of the security of equipment and products for the purposes of national security". Such a system would have to be linked to the provisions on the exercise of "golden power" with regard to products or services that could affect networks inherent to broadband electronic communications services based on 5G technology<sup>629</sup>. The aim was to "deal with any emergency situation in the cyber environment as effectively and quickly as possible", which can make all the difference in mitigating the negative consequences of an attack.

Taking these needs into account, the Perimeter Decree intervened to ensure the achievement of a high level of IT security, complementing what was already being done by the NIS Decree. Despite this similarity, the different purpose of the two interventions should be emphasised. While for the NIS legislation, raising the level of national security was an instrumental objective to contribute to a better protection of European cyber assets, the Perimeter legislation exemplifies the sensitivity of the new role of the state.

Consequently, although the new regulatory framework is certainly complementary to those derived from the European context, it should be emphasised that it differs markedly from the strictly internal purpose of national security. When the State becomes digital<sup>630</sup>, it enters an entirely new dimension which, on the one hand, allows for new and multiple relationships with the citizen, but which, on the other hand, is tantamount to exposing it to a new set of threats to its own continuity and the integrity of its services.

---

peace and stability, with various efforts that have also considered the possibilities offered by new technologies (think of the deep-fake phenomenon). See Elena Lazarou et al., 'Peace and Security in 2022 - Overview of EU Action and Outlook for the Future' (European Parliamentary Research Service, July 2022), 56–56, [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/733605/EPRS\\_STU\(2022\)733605\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/733605/EPRS_STU(2022)733605_EN.pdf); European Commission, 'COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Tackling Online Disinformation: A European Approach', 26 April 2018, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236>; Council of the European Union, 'Council Conclusions on Strengthening Resilience and Countering Hybrid Threats, Including Disinformation in the Context of the COVID-19 Pandemic', 15 December 2020, 13626/20, <https://data.consilium.europa.eu/doc/document/ST-14064-2020-INIT/en/pdf>.

<sup>628</sup> Associazione Italiana per la Sicurezza Informatica, 'Rapporto Clusit 2020 sulla sicurezza ICT in Italia' (Clusit, March 2020), 12, [https://clusit.it/wp-content/uploads/download/Rapporto\\_Clusit\\_2020\\_web\\_marzo.pdf](https://clusit.it/wp-content/uploads/download/Rapporto_Clusit_2020_web_marzo.pdf).

<sup>629</sup> The issue of 5G has not only been heard at EU level, but has also been taken up by Copasir as an element of concern. Please see Comitato Parlamentare per la Sicurezza della Repubblica, 'RELAZIONE sulle politiche e gli strumenti per la protezione cibernetica e la sicurezza informatica, a tutela dei cittadini, delle istituzioni, delle infrastrutture critiche e delle imprese di interesse strategico nazionale', XXXIV (Comitato Parlamentare per la Sicurezza della Repubblica, dicembre 2019), [https://documenti.camera.it/\\_dati/leg18/lavori/documentiparlamentari/IndiceETesti/034/001/intero.pdf](https://documenti.camera.it/_dati/leg18/lavori/documentiparlamentari/IndiceETesti/034/001/intero.pdf).

<sup>630</sup> Pasquale Costanzo, 'Lo "stato digitale": considerazioni introduttive' (Il diritto costituzionale e le sfide dell'innovazione tecnologica, Genova, 2021), 11–36.

The changed context of relations in cyberspace led the legislator to revise the system of bodies set up for the protection of national security<sup>631</sup> with a view to better coordination, both for a more effective exercise of the golden power and for the provision of appropriate safeguards in view of the planned activation of strategic digital infrastructures.

The merit of the resulting organisation lies in its greater degree of specialisation and autonomy compared to the previous intelligence system for the security of the Republic. As proof of this, it is enough to mention the creation, together with other bodies, of an ad hoc national agency, the Agency for National Cybersecurity (ACN [Italian acronym]), which has assumed full coordination at national level, as well as in relations at European and international level.

The new agency is undoubtedly a fundamental building block in the overall simplification of the cybersecurity system. However, the complexity of the issues remains, on the one hand because of the multiplicity of the underlying aspects, and on the other hand because of the "progressive" nature of the legislation, which has required several successive interventions before being completed.

These two aspects are inextricably linked and constitute the starting point for a more detailed analysis of the structure of the perimeter from the point of view of sources, the balance of which is significantly affected by technological development.

Before proceeding with these considerations, it seems useful to define the sources that are of interest, purely from an exploratory point of view<sup>632</sup>. For this purpose, it may be useful to briefly review the structure of the decree, leaving aside the transitional and implementing articles. In general, the decree sets out only the essential principles and obligations, leaving the technical and procedural details to specific decrees of the President of the Council of Ministers. Undoubtedly, the attention should be focused on the first article, which deals with the legal basis for the construction of the security perimeter. Exactly as the now familiar term 'perimeter' promises, the idea behind it is to define the boundaries of the 'digital state', which is now largely characterised by the provision of essential services and functions to citizens<sup>633</sup>.

This means first of all identifying the essential functions of the State and the services on which the exercise of essential services for fundamental civil, social and economic activities depends, among which national security must certainly be included. The next step is to use this knowledge to identify the subjects that are essential to the digital existence of the state and, through them, the ICT assets to be placed within the perimeter. As intelligible as these steps are in the abstraction, the identification of what are known in the jargon as perimeter subjects is not an easy practice, because it requires a strong collaboration between the different actors within the state system.

The precise concretisation of the principles and procedures, in addition to the meagre specifications of the decree, is delegated to a subsequent D.P.C.M., on paper, to be approved within four months of the entry into force of the conversion law. With the usual delay that has characterised the implementation of the Perimeter, D.P.C.M. 131 of 30 July 2020

---

<sup>631</sup> For an essential definition, see the previous paragraph IV.1.

<sup>632</sup> A detailed examination of the individual acts implementing the security perimeter is provided in the Table 1 in appendix I. The following remarks are intended to reconstruct the context of the components from which the compliance requirements for the subjects of the perimeter are derived.

<sup>633</sup> The logic is exactly the same as that of any security perimeter described in appendix I, using the most relevant international standards and guidelines..

delegates the task of the concrete identification of the subjects to various sectoral authorities<sup>634</sup>, which must take into account a series of operational criteria<sup>635</sup>.

Finally, the procedure also regulates the timing of the notification of the subjects of their inclusion in the perimeter. The complete list of perimeter subjects is contained in a non-published D.P.C.M.<sup>636</sup>, whose lack of transparency is offset by the obligation to notify COPASIR of the list of subjects and any updates thereto within ten days<sup>637</sup>.

It should be made clear from the outset that the Perimeter Decree must be read in the light of the subsequent regulatory interventions that have taken place to complete the system. The reference is not only to the secondary sources analysed, but in particular to Decree Law 82 of 14 June 2021, which established the National Agency for Cybersecurity (ACN [Italian acronym]). In this way, the legislator has intervened with a significant simplification, centralising most of the core functions of the cybersecurity system in the new agency, thus emphasising the autonomy of cybersecurity with regard to the information system for the security of the Republic. Consequently, all references to the Ministry of Economic Development, the Presidency of the Council of Ministers and the Department of Information

---

<sup>634</sup> On the one hand, a number of sectoral authorities, each in its own area of competence, must identify the entities, and on the other hand, these entities must be informed of their inclusion and provide a list of their ICT assets necessary for the performance of essential functions or services. See articles 4,5,7,8 of the D.P.C.M. 131 of 2020. The list must then be sent to the Agency for National Cybersecurity (CAN [Italian acronym]). The implication is that not all ICT assets belonging to entities must automatically fall within the perimeter. Only those that serve the essential function or service that the entities perform or enable must be listed. Compare Art. 1 c. 2 lett. b) of D.L. 150 of 2019 and Art. 7 D.P.C.M. 131 of 2020.

<sup>635</sup> The issue of defining the concepts of essential government function and essential service is by no means secondary, since the entire architecture of the perimeter rests on it, determining who is subject to its obligations. Several sets of criteria are defined. Firstly, the continuity of the government and other constitutional bodies, internal security and the defence of the state are emphasised. To these are added other functions commonly regarded as essential to the existence of a civil state, such as the proper administration of justice, the functioning of the economic and financial system, and the transport system. The second set of criteria, on the other hand, is to be found, broadly speaking, in the functionality for the maintenance of civil, social or economic activities that are fundamental to the interests of the state. This formula covers a wide range of activities aimed at the enjoyment of fundamental rights, from the efficiency of supply infrastructures to any activity characterised by economic and social importance for national development and strategic autonomy. All these functions or services, which are cybersecurity, must depend on networks, information systems or computer systems. On the other hand, from an operational point of view, the risk of an incident is considered on the basis of a graded criterion that contextualises the potential damage to national security depending on the specific sector. For example, the territorial extent of the function, the number of users involved, the consequences of an incident, including economic ones, and the possibilities of mitigating them are taken into account. For comparison, see Art. 1 c. 2 let. a) of D.L. 105 of 2019 and Art. 4 of D.P.C.M. 131 of 2020. It should be noted that the criteria also include the activity of constitutional bodies, which are expressly excluded from the application of the perimeter rules. Although they perform functions that are undoubtedly relevant to the State, they remain free to adopt measures and arrangements similar to those of the perimeter subjects, entering into a special agreement with the Prime Minister for this purpose. This agreement is subject to confidentiality.

<sup>636</sup> Compare Article 1 c. 2-bis of D.L. 105 of 2019 and Article 5 of D.P.C.M. 131 of 2020. The first D.P.C.M. listing the subjects is the D.P.C.M. of 25 November 2020, followed by an update on 15 June 2021 by President Draghi. For context, see Luisa Franchina, Andrea Lucariello, and Francesco Ressa, 'Ampliamento del perimetro di sicurezza nazionale cibernetica: ecco i settori di attività', *Agenda Digitale*, 18 June 2021, <https://www.cybersecurity360.it/cybersecurity-nazionale/ampliamento-del-perimetro-di-sicurezza-nazionale-cibernetica-ecco-i-settori-di-attivita/>.

<sup>637</sup> Compare Art. 1 c. 2-ter of D.L. 105 of 2019.

for Security should be understood as referring to the ACN<sup>638</sup>. The same applies to all the specific cybersecurity bodies created to relieve and replace the bodies established by Law 124 of 3 August 2007<sup>639</sup>.

Following on from the analysis in this first article, two other key groups of issues can be identified. The first relates to the main compliance obligations of operators of essential services, namely the obligation to notify incidents affecting perimeter assets and the obligation to implement adequate security measures to ensure a high level of security<sup>640</sup>.

The second concerns the provisions for the activation of the CVCN<sup>641</sup> and the procedure for controlling the procurement of ICT goods, systems and services for use on perimeter assets<sup>642</sup>.

As each of these issues has been referred to in a secondary source, it is best to follow the chronological order.

The second measure concerns the procurement of ICT goods, systems or services to be used within the perimeter. In these cases, entities must notify the National Evaluation and Certification Centre (CVCN [Italian acronym]), a body strengthened by the Perimeter Decree also for a refinement of the Golden Power regulation, recently extended to the scope of broadband electronic telecommunications networks with 5G technology. The CVCN plays an essential role for the President of the Council of Ministers, as it enables him to assess the prudent exercise of the special powers on the basis of a technical analysis resulting from a series of tests, the passing of which is a necessary condition for the effectiveness of the award.

However, the possibility of assessing the technical profile is not only functional for the purposes of the Golden Power, since it fits into the broader framework offered by the Perimeter, whose legislative decree postpones the definition of all verification procedures to a regulation to be adopted within ten months of the entry into force of the conversion law.

Therefore, D.P.C.M. n. 54 represents the second pillar of the National Perimeter's implementation, following D.P.C.M. n. 131. Although further political and legal interventions were required to fully activate CVCN (in Italian "Centro di Valutazione e Certificazione Nazionale")<sup>643</sup>, it nonetheless established the foundations for the development of procedures

---

<sup>638</sup> See Article 1 of D.L. No 82 of 2021, as amended by L. No 109 of 4 August 2021.

<sup>639</sup> This refers, for example, to the Cybersecurity Unit, which assumes all the tasks previously assigned to the Cybersecurity Unit by the Perimeter Regulation, or to the Interministerial Committee on Cybersecurity, which assumes all the functions of the Interministerial Committee on the Security of the Republic.

<sup>640</sup> Compare Art. 1 c. 3,4 of D.L. 105 of 2019.

<sup>641</sup> The CVCN as defined in Art. 1 c. 7 of the Decree Perimeter: a) contributes to the elaboration of security measures for the procurement of ICT goods, systems and services; b) verifies the security conditions and the absence of known vulnerabilities, defining verification and testing methodologies and, where appropriate, prescribing the use to the customer; c) develops and adopts cyber certification schemes, taking into account standards defined at international and European Union level, when, for national security reasons, existing certification schemes are not considered sufficient to meet the protection needs of the national cyber security perimeter. A full list of the functioning of the CVCN can be found in Table 1 in appendix I.6.

<sup>642</sup> Compare Art. 1 c. 6,7 of D.L. 105 of 2019.

<sup>643</sup> As seen in the previous paragraph, the CVCN had been established at the Ministry of Economic Development in implementation of Article 11 c. 2 of the Prime Ministerial Decree of 17 February 2017. It had been established by the Decree of the Minister of Economic Development of 15 February 2019, but both resources and personnel were insufficient to cope with the new testing activities assigned by the perimeter regulations.

for the technological assessment of ICT assets.

If D.P.C.M. 131 outlined the extension of the Perimeter, defining the principles for identification of both the perimeter subjects and their ICT assets, D.P.R. 54 can be deemed as the gatekeeper of what can and cannot enter the Perimeter. As the subject's needs change, they are forced to acquire new technologies or ICT services, which can directly or indirectly affect their security. When the object of a procurement might have an impact on the Perimeter, the final decision about the adjudication and the subsequent choice of the supplier cannot only be based on cheapness but had to consider the inherent security. Therefore, D.P.R. 54 aims to ensure that only secure assets, systems, and ICT services can be part of the Perimeter.

The decree, in fact, contains the procedures, modalities, and deadlines for evaluations by the CVCN and CVs. The beginning of the procurement process for a perimeter subject must be communicated to CVCN in order to allow it to carry out some preliminary checks. The identification of the technical requirements for inclusion in the announcement or contract is a crucial step in the procurement process, as they serve as binding obligations for both the procuring organization and potential suppliers. After the adjudication, the CVCN is informed about the status of the procurement process and determines a plan to execute the tests, if they have not already been performed on the same object. As a result, the awardee has to provide the object of the procurement for the tests. The CVCN, a CV (in Italian “Centro di Valutazione”) or a LAP (in Italian “Laboratorio di Prova”) draws up a report of the tests, which is used by the CVCN for the final evaluation report. Depending on whether the outcome of the procedure is positive or negative, the final award can be allowed, allowed with certain obligations to use, or denied.

Not all procurement processes initiated by perimeter subjects must be submitted to the control of CVCN, but only those whose objects are within specific categories, which are covered by the D.P.C.M. of June 15, 2021. The identification of these categories, in compliance with the criteria of article 13 of D.P.R. 54 is the second fundamental content of the discipline in question.

Finally, the procedures, methods, and deadlines by which the competent authorities carry out verification and inspection activities are identified<sup>644</sup>.

However, this infrastructure still lacked some essential steps. The full activation of the CVCN required the allocation of adequate resources and personnel, as well as the identification of premises and infrastructure for carrying out testing activities. There is no hiding the long period of stalemate that characterised the start of testing activities. Decree Law No. 82 of 2021 provided a major boost. After a deadlock that had lasted since 2019, the creation of the Agency for National Cybersecurity had also provided an opportunity to address the timing of the implementation of the perimeter regulation, setting 30 June 2022 as the deadline for the first operation of the certification system<sup>645</sup>. After a gradual transfer of

---

<sup>644</sup> As already mentioned above, although the original text of the decree refers to different competent authorities, it must be noted that the discipline must be interpreted considering the subsequent D.L. 82 of 2022, which established the Italian Agency for National Cybersecurity. Therefore, all references to the Presidency of the Council of the Ministry and the Ministry of Economic Development must be interpreted in light of the establishment of the new agency.

<sup>645</sup> Art. 16 c. 9 let. a) of D.L. 82 of 2021 had in fact specified: "The reporting obligation referred to in this letter shall take effect as of the thirtieth day following the publication in the Official Gazette of the Italian Republic of the Decree of the President of the Council of Ministers certifying, after consultation with the Agency for National

personnel and facilities to the ACN, the Decree of the President of the Council of Ministers of 15 June 2022 authorised the final transfer of the CVCN and its activation on schedule.

After the topic of technological control of the security of ICT goods and services, the third measure dealt with the definition of the bulk of the compliance obligations to which perimeter actors are subject. After D.P.R. 54, D.P.C.M. 81 (D.P.C.M. 2, as usually referred to by experts) is the third pillar of the Perimeter and one of its most technical components. These aspects outline a duplicity of aspects, which overall follows those essential components that have always characterized security since the first regulations attempted to control the development of information technologies in their different declensions. There are, in particular, many similarities with the NIS directive system, which is also partially utilized by the Perimeter.

Incidents notification to the CSIRT (Computer Security Incident Response Team) is the first main obligation on perimeter subjects<sup>646</sup>. While initially an experimental practice, it has become mandatory since January 1, 2022. The decree contains two attachments. Attachment A defines a taxonomy of the incidents that can affect assets within the Perimeter and have to be promptly notified. According to the different severity level of the incidents, two different timings are established. The notification must include the definition of the incident provided by the taxonomy, as well as all the necessary elements to describe significant features related to the security event. Additional information may be required by the CSIRT.

The importance of providing security-related information has increased significantly since the start of the Ukraine war, which is why the so-called “Decreto Aiuti Bis” (D.L. 115 of 9 August 2022) has been enacted to expand the notification to include a broader range of incidents. An amendment to the D.L. 105 of 2019 mandated notification of incidents influencing assets outside the Perimeter. The new obligation has been complemented by a new taxonomy of incidents, published with the resolution of the general director of the Agency for National Cybersecurity.

In addition to the value of the information obtained from the knowledge of the incidents, there is an increase in security, imposed according to a progressive implementation, to complete the categories simply listed by the Perimeter Decree. The logic is that of the initial implementation of the minimum level of security, to then increase the protection in the medium term. The fundamental difference with other regulations, however, lies in the direct inclusion of the specific measures to be adopted, without resorting to generic formulas, which would have implicitly led to the adoption of the most recent guidelines in any case<sup>647</sup>.

---

Cybersecurity, the operability of the CVCN, and in any case as of 30 June 2022".

<sup>646</sup> As for the other decrees, the interpretation of D.P.C.M. 81 is influenced by the subsequent decree 82 of 2022, which established the Italian Agency for National Cybersecurity. Therefore, all the references to the DIS (Department of Security Information or in Italian “Dipartimento delle informazioni per la sicurezza”) have to be interpreted in relation to the new agency. Furthermore, since the ACN has acquired the CSIRT, all requirements regarding the relay of incident notifications to the Ministry of Economic Development and the Presidency of the Council of the Ministry must be ignored.

<sup>647</sup> Annex B of D.P.C.M. 81 of 14 April 2021 has two annexes. The first one contains a table with the security measures per category. The second defines the level of priority in the implementation of the above-mentioned measures. Appendix C, on the other hand, concerns the minimum security measures for the protection of information. Article 8 of the D.P.C.M. in question establishes three levels of priority, each starting from the notification referred to in art. 1 c. 2 let. b) of Legislative Decree no. 105 of 2019, i.e. the notification of the list of networks, information systems and IT services, including architecture and components, that each entity must send to ACN within six months of receiving the notification of inclusion in the perimeter referred to in art. 1 c.

The last piece to complete the perimeter is the criteria for the accreditation of testing laboratories and evaluation centres to support the technical activities of the CVCN. In order to relieve the CVCN's testing activities, it is planned to establish a support network distributed throughout the country to which most of the operational activities can be delegated. In order to set up this network, it was necessary to define specific accreditation criteria and procedures to ensure that the laboratories meet minimum reliability criteria. This, as well as the links and exchange of information between the CVCN, CV and LAP, is provided for by Decree of the President of the Council of Ministers No. 92 of 18 May 2022<sup>648</sup>.

The Figure 24 summarises the regulatory steps just described and shows the basis within the Perimeter Decree.

---

2-bis of the D.L. Within thirty days, the minimum security measures set out in Annex C must be implemented, within six months for those identified as belonging to category A, and finally within 30 months for those belonging to category B. The implementation of the measures set out in Annex B must be communicated to the ACN.

<sup>648</sup> The D.P.C.M. deals with the procedures, modalities and deadlines to be followed both for the accreditation of CVs and testing laboratories and for the management of the respective links with the CVCN and the CVs. The CVCN is the accreditation authority that defines the technical requirements, security measures and competences that laboratories must have in order to be accredited (Article 4 of the D.P.C.M.), as well as the areas for which accreditation can be requested (Article 7 of the D.P.C.M.). LAPs are required to implement appropriate security measures and to report security incidents (Article 22 of the D.P.C.M.). The CVCN has a special Accreditation Commission to support its activities (Article 5 of the D.P.C.M.). As the competent authority, the CVCN also carries out supervisory functions to ensure compliance with the obligations and requirements of the LAPs by means of spot checks and inspections (Article 14 of the D.P.C.M.). The accreditation procedure is described in detail in its phases (art. 12 of the D.P.C.M.), starting with the application with all its contents (art. 10, 11, 20 of the D.P.C.M.) and the requirements, both objective (art. 8 of the D.P.C.M.) and subjective (art. 9 of the D.P.C.M.). The procedures for renewal (art. 16 of the D.P.C.M.) or any modification of the certification (art. 17 of the D.P.C.M.) are also defined. In order to ensure an effective exchange of information, the CVCN keeps a computerised register of tested IT assets (art. 21 of the D.P.C.M.).



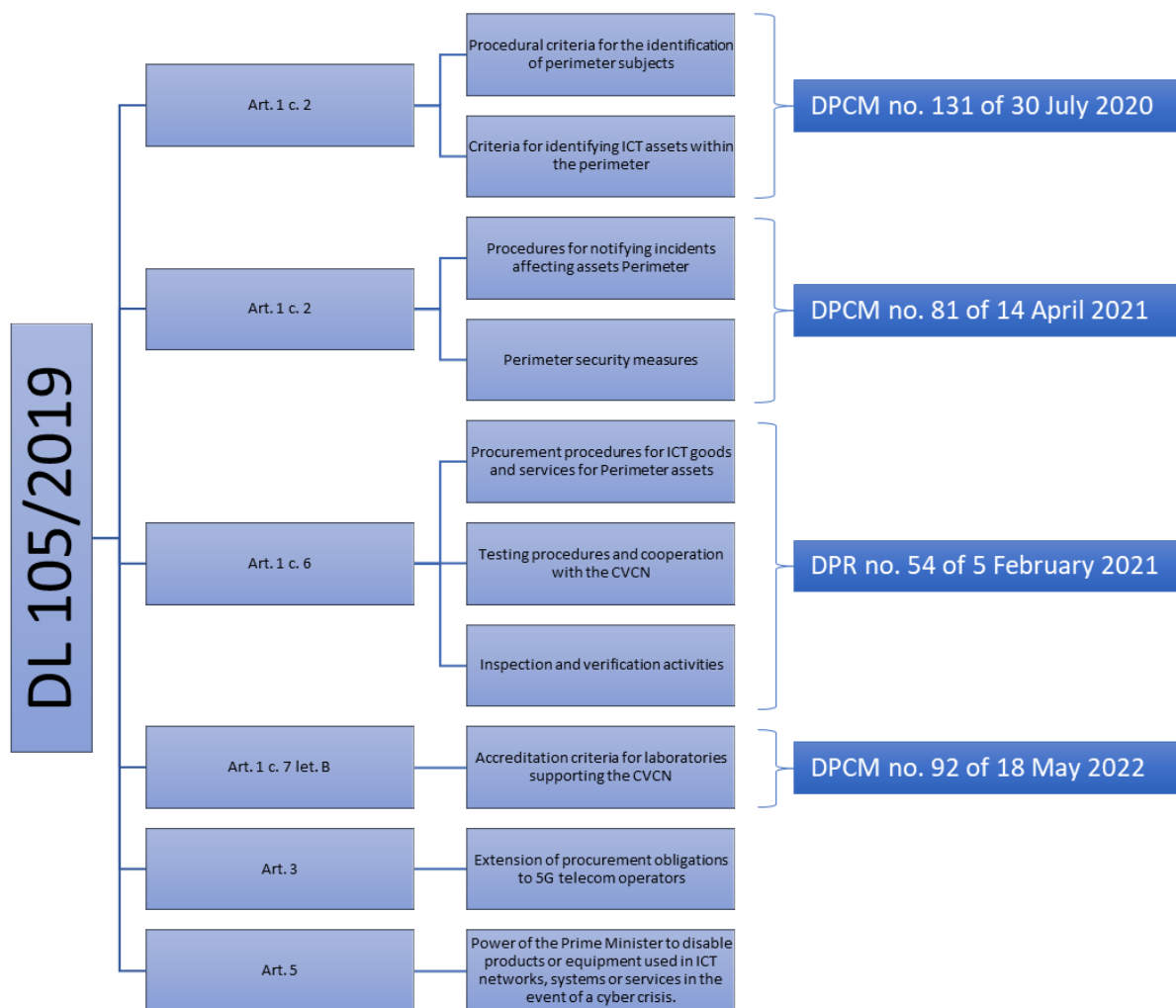


Figure 24 - National Cybersecurity Perimeter's foundations

Article 1, in its various sub-paragraphs, contains the principles for the establishment of the security perimeter and its legal basis. Each relevant article and paragraph are shown in Figure 24, together with a summary of its content. On the side, the secondary legislation based on the various paragraphs of Article 1, as mentioned above, is shown.

At the same time, Figure 24 highlights the other relevant articles within the scope of the Perimeter Decree. Although they do not have a direct impact on the structure of the perimeter, it is worth taking a brief look at them.

As expected, the discipline of the so-called "golden power" benefits greatly from the instruments of the perimeter, in particular from the creation of the CVCN, which does not remain an instrument dedicated only to the subjects of the perimeter.

Following the reform of the special powers introduced by Decree-Law 21 of 15 March 2012, in order to remedy the previous situation of incompatibility with the EU system<sup>649</sup>, a

<sup>649</sup> For reasons of practicality and context, it is not possible here to reconstruct all the regulatory steps in the field of Golden Power, or rather Golden Powers. For anything not directly related to cybersecurity, including older regulatory developments, please refer to Pierluigi Di Palma and Francesco Gaspari, 'L'attuazione Del "Golden Power" in Italia: Dal Potere Regolamentare Alla Potestà Regolatoria', *GiustAmm.It*, no. 4 (2013): 40; Elisabetta Freni, "'Golden Share': Raggiunta La Compatibilità Con l'ordinamento Comunitario?", *Giornale Di Diritto Amministrativo*, no. 1 (2013): 25–33; Andrea Sacco Ginevri, 'I "Golden Powers" Dello Stato Nei Settori Strategici Dell'economia', *Federalismi.It*, no. 22 (2016): 14.

number of secondary laws had intervened to define the activities of strategic importance and the procedures for activating the powers in the various sectors<sup>650</sup>.

In particular, Decree Law 22 of 25 March 2019 extended the Golden Power to all broadband electronic communications services based on 5G technology<sup>651</sup>. In this respect, the CVCN constitutes an effective control instrument at the disposal of the President of the Council of Ministers to decide on the application or non-application of the special powers. Article 3 clarifies that all entities intending to proceed with the acquisition, for whatever reason, of goods, services and components related to broadband electronic communications services based on 5G technology are obliged to follow the technical verification procedures set out in Presidential Decree 54. On the other hand, the suppliers of the goods and services must provide the CVCN with their full cooperation in carrying out the verification activities.

As a result, this organisation guarantees an improvement in cyber protection that goes beyond the security perimeter and has a more pervasive effect.

The result is improved protection in cases where both regulations apply, i.e. when perimeter actors need to purchase 5G goods or services. In reality, however, it is difficult to imagine a situation where an acquisition of 5G technologies would fall outside the security perimeter, i.e. be made for assets outside the perimeter.

The last element concerns the power of the President of the Council of Ministers to respond to a cyber crisis by ordering the total or partial disablement of one or more devices or products used in the networks, systems or for the provision of the services concerned. Of course, the exercise of this power must be accompanied by appropriate safeguards, which require a strict balancing with other fundamental rights. Accordingly, the disconnection must be indispensable for the purpose of mitigation and must be carried out for the time strictly necessary, in accordance with a criterion of proportionality. In addition to these restrictions, it should be noted that this is not a power that can be freely exercised by the Prime Minister. At the time of the conversion of the Decree-Law, the obligation of prior consultation of the Interministerial Committee for the Security of the Republic, which has been involved in national crisis management since the intervention of Legislative Decree 174 of 30 October 2015, was introduced<sup>652</sup>. In addition, COPASIR must be duly informed of any exercise within 30 days.

At the end of this entire examination, the Figure 44 in appendix IV summarises all the relevant legal acts mentioned in this paragraph.

---

<sup>650</sup> D.P.R. 85 and 86 of 25 March 2014 had intervened to identify assets of strategic importance and the procedures for activating powers in the energy, transport and communications sectors, respectively. Subsequently, the Prime Minister had addressed the defence and national security sectors with D.P.C.M. 35 of 19 February 2014 and 108 of 6 June 2014. Article 14 of Decree-Law 148 of 16 October 2017 had intervened in these initial sectors to extend the exercise of powers to critical infrastructure, critical technologies and critical supplies.

<sup>651</sup> Article 1 of Decree Law 22 of 25 March 2019 introduced Article 1-bis into Decree Law 21 of 2012, which is dedicated to special powers regarding broadband electronic telecommunications networks with 5G technology. The so-called Ukrainian Decree (Decree-Law 21 March 2022) also intervened in these changes. 'As a consequence of the crisis in Ukraine and in order to prevent possible damage to national security in cyberspace, the same administrations shall immediately diversify the products used' [author's translation].

<sup>652</sup> While the work of the CISR was initially supported by the "nucleo per la sicurezza cibernetica", these cybersecurity tasks have been transferred to the new "nucleo per la cybersicurezza" created after the creation of the ACN within the Agency itself. See Article 8 of Decree Law 82 of 2021.

## V Direct Insights into the Cybersecurity Perimeter of Constitutional Bodies: A Questionnaire-based Study

In line with the multi-level view with which the regulation of a complex issue such as cybersecurity has been approached, this final analysis aims to focus on a particular internal perspective.

The previous chapter introduced the various components that make up the National Security Perimeter. Of fundamental importance is DPCM 1, which defines the boundaries of the perimeter and the subjects to which it applies. In very broad terms, reference is made to the concepts of essential government functions and essential services, which are in turn specified by a number of examples. The first refers precisely to the continuity of the government and other constitutional bodies, internal security and the defence of the State.

Although a careless reading of the provisions could lead to the inclusion of Constitutional bodies within the perimeter, Article 2(2) of D.P.C.M. 131 of 30 July 2020 expressly excludes this automaticity.

As a result, all entities supporting the constitutional bodies are inside the security perimeter, while the constitutional bodies are outside<sup>653</sup>.

The reason for this is to preserve the separation of powers and to guarantee the autonomy and independence of these fundamental bodies, including with regard to their own cybersecurity decisions.

Without corrective action, such an organisation would certainly end up contradicting some of the most basic functions of cybersecurity. Think of the important role of standardisation<sup>654</sup> or the need for networking and constant exchange of security information. The open and collaborative nature of this branch of security means that no actor can meet its needs alone, unless it is faced with prohibitive costs and hard-to-find skills.

Probably aware of these undeniable needs, the President of the Council of Ministers had left open the possibility of participating in the security Perimeter on a voluntary basis. Each constitutional body can freely decide to enter into special agreements with the President to adopt security measures similar to those provided for by the Perimeter. One can imagine that the reference to the implementation of security measures is to be understood as including the entire support network available on the basis of the entire institutional infrastructure.

---

<sup>653</sup> Initially, the text of the D.P.C.M. made no reference to constitutional bodies, which were only mentioned in the definition of an essential service: [my translation] "a subject performs an essential function of the State [...] when the legal system assigns to it tasks aimed at ensuring the continuity of the action of the Government and the constitutional bodies". It was precisely the Council of State that, in its opinion on the draft D.P.C.M. 131, had pointed out the complexity of correctly defining the boundaries of the Perimeter. It had highlighted the confusion in the definition of what was an essential service. In the absence of clarification to the contrary, constitutional bodies should have been included within the perimeter, as they were certainly entrusted with an essential function of the State. It correctly stated that [my translation] "constitutional bodies cannot be included, *sic et simpliciter*, for fear of compromising their constitutionally guaranteed sphere of autonomy and independence". See Consiglio di Stato, 'Schema di decreto del Presidente del Consiglio dei ministri (d.P.C.M.) in materia di perimetro di sicurezza nazionale cibernetica, adottato in attuazione dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133', 21 May 2020, 12, [https://www.giustizia-amministrativa.it/portale/pages/istituzionale/visualizza/?nodeRef=&schema=consul&nrg=202000417&nomeFile=202000983\\_27.html&subDir=Provvedimenti](https://www.giustizia-amministrativa.it/portale/pages/istituzionale/visualizza/?nodeRef=&schema=consul&nrg=202000417&nomeFile=202000983_27.html&subDir=Provvedimenti). (Council of State, 2020, p. 12).

<sup>654</sup> See chapter **Error! Reference source not found..**

Of course, the extent and level of integration within the Perimeter remains a choice for individual institutions, exercising their prerogatives of autonomy and independence<sup>655</sup>.

It can be assumed that the constitutional order has extended its institutions to include the security needs of constitutional bodies in a broader sense.

Attempting to keep the discourse general, without referring to the specific situation of individual constitutional organs, it is nevertheless possible to categorise prerogatives on the basis of the purpose of their enhanced protection<sup>656</sup>.

Despite the scarcity of doctrinal insights on a topic as new as cybersecurity, it is possible to formulate some considerations based on the organisational prerogatives of constitutional bodies.

In general terms, these can be understood as the definition of rules that allow them to remain institutionally shielded from intervention by other subjects of the legal system. Unlike immunity mechanisms, independence is not achieved by creating obstacles to internal interference<sup>657</sup>.

Independence is the result of the introduction of procedures which, by their very nature, exclude the competences of external bodies.

The proliferation of IT tools, which now characterises aspects of the work of these bodies, opens several doors to possible external dependencies. As with all activities, digitisation means creating a potential attack surface. On the one hand, it is necessary to implement appropriate security measures for IT assets. On the other hand, relationships with potential suppliers of products or services must be managed to ensure that supplies meet certain security standards. Although the problem is mitigated to some extent by the fact that any subordinate party to the organisation should automatically fall within the security perimeter, the need for security must be properly communicated. This implies the provision of adequate resources, both financial and human.

With regard to relations with third parties, the issue of self-determination arises. A whole

---

<sup>655</sup> The term prerogative is used here to refer to a category within the broader set of constitutional guarantees. These are defined by Galeotti as [my translation] “all those mechanisms of legal security which the constitutional order provides in advance in order to safeguard and defend the integrity of its normative value, in other words its very existence”. See Gian Franco Ciaurro, ‘Prerogative Costituzionali’, in *Enciclopedia Del Diritto* (Giuffrè Francis Lefebvre, 1986), 5.

<sup>656</sup> According to established reconstructions, it is possible to speak of prerogatives that can be exercised by constitutional subjects, organisational prerogatives and prerogative situations. The first category includes, for example, the substantive powers of the President of the Republic or the judicial powers of parliamentary investigatory commissions. The second category, on the other hand, refers to the conditions necessary for the functioning of each constitutional body. These include the ability to manage its own internal rules and finances, to decide on internal conflicts and to verify the qualifications of its members. The last category relates to the defence of certain conditions of freedom and security, protected by special conditions of inviolability, irresponsibility, unquestionability or immunity granted to persons belonging to the body or representing it. Inviolability can also be attributed to the premises of the institution, as in the case of the Chambers, which cannot be entered by the public authorities without the express authorisation of the President. The same is provided for in the regulations of the Constitutional Court. See Balladore Pallieri, *Diritto costituzionale*, Giuffrè, 1953, 210; Costantino Mortati et al., *Istituzioni di diritto pubblico*, 10a ed, Manuali di scienze giuridiche (Padova: CEDAM, 1991), 520.

<sup>657</sup> For matters of expediency, please refer to the discussion of ‘L’esonazione Totale dalla Giurisdizione: Immunità dei Capi di Stato e Insindacabilità Parlamentare’, in *Le immunità della politica contributo allo studio delle prerogative costituzionali* (Torino: G. Giappichelli, 2005), 139–203.

body of jurisprudence has developed on this issue, particularly with regard to the parliamentary institution<sup>658</sup>.

### V.1 The experimental activity

Given the difficulty of dealing with an issue that is as topical as it is marginalised by most, an experimental approach to the problem was chosen. In line with the research carried out

---

<sup>658</sup> The starting point for all considerations is the Constitutional Court's decision 129 of 1981. In it, the Court created self-determination out of the normative autonomy granted to constitutional bodies. To quote the key passage of the ruling: the autonomy of constitutional bodies "is not exhausted in the regulation, but includes - coherently - the moment of application of the rules themselves, including the choices regarding the concrete adoption of measures to ensure their observance. [...] Self-determination is a development of the normative autonomy that the Constitution explicitly or implicitly recognises for the Chambers and the President of the Republic". In the 1980s, this prerogative was still justified by the Court as "guaranteed independence", mainly on historical grounds (Constitutional Court decision 154 of 1985). This apparently granitic position was followed by other recent pronouncements. These had laid the foundations for an argumentation in the field of positive law, not unlike what had already been done for the compensation of members of parliament, guaranteed by Article 68(1) of the Constitution. In line with the proposals of part of the doctrine, the Court had given an interpretation of self-determination according to a functional link (Judgment 120 of 2014). Self-determination must be what is strictly necessary to guarantee the free exercise of parliamentary functions. The only body that can decide on the basis of these alleged violations must be the Constitutional Court, in the context of the conflict of attributions between the powers of the State. On the basis of this elaboration, the Court once again decided to introduce new limits to self-determination in Decision 213 of 2017. While self-determination may concern the employment relationship of constitutional bodies with their employees, it cannot go so far as to affect the subjective situations of third parties. The situation of third parties must be protected before the ordinary courts. This state of affairs has been the subject of several doctrinal criticisms. Firstly, it is impossible to prevent the regulatory autonomy of the Chambers from having a slight impact on the situation of third parties. Think of the candidates in public competitions or the public attending hearings. Second, regulatory autonomy does not always mean self-determination. For more details, see Clarice Delle Donne, 'Autodichia Degli Organi Costituzionali e Universalità Della Giurisdizione Nella Cornice Dello Stato Di Diritto: La Corte Costituzionale Fa Il Punto', *Rivista Trimestrale Di Diritto e Procedura Civile*, no. 1 (2015): 141-64; Renato Ibrido, "In Direzione Ostinata e Contraria". La Risposta Della Corte Costituzionale Alla Dottrina Della Sindacabilità Dei Regolamenti Parlamentari', *Rivista AIC*, no. 3 (2014): 3; Nicola Lupo, 'Sull'autodichia La Corte Costituzionale, Dopo Lunga Attesa, Opta per La Continuità (Nota a Corte Cost. n. 262 Del 2017)', *Forumcostituzionale.It* (blog), dicembre 2017, [https://www.forumcostituzionale.it/wordpress/wp-content/uploads/2017/11/nota\\_262\\_2017\\_lupo.pdf](https://www.forumcostituzionale.it/wordpress/wp-content/uploads/2017/11/nota_262_2017_lupo.pdf). For the sake of context, we prefer not to go into further procedural aspects involved in this case. One example is the applicability of the jurisdictional rules of the Court of Cassation. For further information see Clarice Delle Donne, 'La Questione Di Autodichia Nel Processo (Ovvero Degli Incerti Confini Tra Regolamento Di Giurisdizione e Conflitto Di Attribuzioni)', *Judicium*, no. 3 (2020): 10-18. This whole parenthesis serves to introduce one of the last passages of the case, which is relevant from the point of view of IT security. On the basis of the above-mentioned developments in constitutional jurisprudence, the Council of State considered the question of relations with third parties. If, in principle, self-determination can only concern situations of an internal nature, it is necessary to consider on a case-by-case basis which cases fall within the jurisdiction of the constitutional body or the ordinary courts. In the past, the Court of Cassation confirmed that the issue of life annuities falls within the competence of autodichy. See Luca Castelli, *L'autodichia Degli Organi Costituzionali: Assetti, Revisioni, Evoluzioni*, Per Una Koiné Costituzionale 12 (Torino: G. Giappichelli Editore, 2019), 215. The Council of State, on the other hand, had dealt with procurement disputes between the constitutional body and third parties. Taking up the few references of the 2017 judgment 262 on procurement, it had clearly reaffirmed the removal of the matter from self-determination. This automatic referral to the ordinary court would run the risk of ignoring the complex issues involved. For a detailed critique of the judge's reasoning, see Tino Iannuzzi, 'La Corte Costituzionale è Il "Giudice Naturale" Della Autodichia. Nota Alla Sentenza Della Quinta Sezione Del Consiglio Di Stato n. 4150 Del 31 Maggio 2021', *Federalismi.It*, no. 28 (2021): 70-75. The author concludes by stressing that the conflict of attributions between the powers of the State should be the preferred instrument for assessing the specific relationship with third parties on a case-by-case basis. In any case, the Constitutional Court should have the last word. This is especially true in a sensitive matter such as public procurement.

as part of the ERACLITO project, a research question was posed to complete the Perimeter. The aim was to examine the relationship between the Constitutional Bodies and the Perimeter. The initial hypothesis was that there would be a more or less pronounced impact on autonomy and independence due to the impossibility of fully internalising the security functions required by law for the subjects of the perimeter. In this sense, the question arises as to whether the Perimeter can also be a good internal reference standard for these subjects, even if they are not bound by its rules.

The research began after a careful study of the Perimeter legislation in order to outline a series of questions to be administered to each of the constitutional bodies. Special thanks are due to the initial contribution of ACN's Legal, Legislative and Regulatory Affairs Department, which provided assistance in identifying key issues.

The questionnaires were divided into eight sections.

The first deals with the specific arrangements for joining the Perimeter. In particular, the aim is to explore the nature of the membership agreements and the extent to which they can be made transparent. The expectation is to be able to trace the trend of the institutions towards the Perimeter, i.e. whether they welcomed it or opted for autonomous solutions. In this respect, compliance is the preliminary question for further research.

In general, the aim is to map the extent to which the Constitutional Bodies have decided to use the Perimeter. Accordingly, in sections 2 to 6, a series of targeted questions are proposed, aimed on the one hand at assessing the degree of integration with the perimeter, and on the other hand at assessing the extent to which its introduction really represents an innovation compared to the previous situation. Questions range from the census of assets and their selection criteria to the security measures adopted. The issue of security supplies and services is not overlooked, which is important for the technological checks to be carried out by the CVCN to ensure the correct application of Golden Power. Particular attention is paid to the relationship between the CVCN and the ACN, which has inspection and control powers.

Finally, the final sections focus on security resources, both in terms of budget and staff skills. In this way, an attempt is made to measure the level of awareness of cyber risks among the institutions. It also takes into account exchanges between constitutional bodies and other relevant actors within the national system.

The questionnaires have been administered in the Constitutional Bodies since September 2022, in some cases requiring more details. The distribution was accompanied by a privacy policy for the management of the data collected. Due to the sensitivity of the issues covered, respondents requested anonymity.

In addition, the use of the data collected was conditional on the anonymisation of the results. To the detriment of the quality of the work, it is not possible to make a comparison between the security practices of one Constitutional Body and another. Precisely in order to avoid any possible comparison, it is also not possible, due to the small number of institutions surveyed, to specify which institutions agreed to answer the questions in full or in part. In view of this limitation, it is preferable not to publish the questions and answers submitted in full<sup>659</sup>. In the interests of maximum cooperation with the institutions involved and scientific

---

<sup>659</sup> Although no classified material has been handled during the research, it is not uncommon to stumble on classified information during this kind of research activity. It must be kept into account that information about security incidents, threats, security procedure and practices adopted by an organisation are usually classified

fairness, the research is in no way intended to be a risk assessment of the central state administration. As already stated, the perspective is that of the relationship between the perimeter and these particular organs of the state, without this leading to an assessment of their security posture.

What follows is an attempt to summarise the main findings of the interviews, following the order of the sections.

#### V.1.1 The Agreements

The first question concerns membership arrangements in the Perimeter. As the interviews took place over a relatively long period, a slightly different situation was captured for each institution. This was a symptom of the different stages of development of the activities in preparation for joining the Perimeter.

Despite the fact that Article 2(2) of D.P.C.M. 131 mentions the President of the Council of Ministers, once the ACN was established it was conceivable that the agreements would have the new agency as the interlocutor. All the interviewees had confirmed the existence of ongoing negotiations with ACN to define its level of integration.

Some ongoing situations were confirmed by the subsequent publication of an agreement with the agency. At the time of writing, several central administrations had concluded an agreement<sup>660</sup>. These include the Chamber and Senate agreements signed in January and December 2023 respectively.

Although it is conceivable that more agreements will be published in the coming months, it is important to remember that these are always delicate processes. Consequently, it cannot be taken for granted that every institution will always opt for transparency. In general, it is possible to confirm a strong focus on cybersecurity, but not the approach to publicising such efforts. Usually, publicity follows a period of consolidation and work to avoid excessive attention or, worse, interference in internal processes. Obviously here reference is made to the mere news of the existence of an agreement with ACN.

#### V.1.2 Adaptation to the technological standard

The following sections open up an investigation of a technological nature into the security practices used. The first perspective that cannot be taken for granted is that of the existence or non-existence of essential services that depend on information networks or services. In fact, not all organisations use digital tools in the same way to perform their essential functions. Some simply use IT support tools, but these do not characterise the institutional work of the institution. From the point of view of continuity, an attack on these assets would have few consequences in terms of functionality. What is more interesting, however, is the existence of tailor-made services that are not limited to mere support, but are essential for

---

information. The handling of classified information is regulated by Presidente del Consiglio dei Ministri, 'DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 12 giugno 2009, n. 7/2009 - Determinazione dell'ambito dei singoli livelli di segretezza, dei soggetti con potere di classifica, dei criteri d'individuazione delle materie oggetto di classifica nonché dei modi di accesso nei luoghi militari o definiti di interesse per la sicurezza della Repubblica', 12 June 2009, <https://www.parlamento.it/documenti/repository/commissioni/bicamerali/COMITATO%20SICUREZZA/DPCM%2012%20GIUGNO%202009%20N.7.pdf>. Even the lowest classification level requires the use of isolated ICT resources in certified environments. Due to the sensitive nature of the research, stricter censorship of the information is preferable to avoid any potential harm to the interviewee.

<sup>660</sup> According to the ACN Press Office, the Bank of Italy, ANAC, ACCREDIA and Consip S.p.a. signed a memorandum of understanding to benefit from the services offered by the Agency. See the press releases published on ACN's website.

carrying out activities.

Consequently, two different levels of digital assets can be identified, as is usually the case with perimeter subjects. Only the second, those that prepare an essential function or an essential service, are those that should be placed under stricter protection and therefore included in the Perimeter. The use of the conditional in this case is a must, as respondents point out that there is no real obligation for the Constitutional Bodies to draw up a list of assets to be communicated to the ACN.

However, it should be stressed that the absence of a sanctioned obligation does not mean inertia. The feedback has been very positive, with all the institutions claiming, albeit to varying degrees, that they have for some time been conducting a census of their IT networks and systems. This allows them to identify their own personal security perimeter or even several perimeters, depending on their importance.

Even if the census does not follow the guidelines prescribed by the Perimeter Regulation, its characteristic features remain. For example, an impact assessment is used to introduce mitigation measures proportionate to the level of risk. The risk assessment is repeated over time to update the lists. This process pays particular attention to external dependencies. This is all the more necessary when it is not possible to provide the necessary services independently.

The subject of outsourcing services is of interest because the special nature of constitutional functions has often gone hand in hand with their digitalisation. As one can imagine, over time, institutions have equipped themselves with special systems to improve the performance of their activities. These are not simply support services, but real services tailored to the performance of their core functions. Without going into specifics, it is possible to refer to all those operations in which representative bodies exercise their mandate. Both the Chamber of Deputies and the Senate of the Republic have a common need to collect the results of the votes cast by their members.

This is done by means of systems specifically designed for this purpose, which must at the same time ensure that the texts of the meetings are handled with the appropriate degree of secrecy when the principle of publicity of the proceedings does not apply. A similar problem has recently arisen for the Constitutional Court with the introduction of its telematic procedure. Its implications concern not only the handling of self-generated information, but also information relating to persons wishing to have access to the constitutional process. Moreover, it must be borne in mind that the information handled in this context may also be classified, since the Constitutional Court is the only court against which state secrecy cannot be invoked. It follows that the system must be set up with these specific security needs in mind<sup>661</sup>.

---

<sup>661</sup> A specific analysis of the comparative security of parliaments has already been carried out in the past, outlining the importance of cybersecurity for these Constitutional Bodies. Its considerations can, by extension, be applied to the present discourse. In particular, five categories of information potentially processed by constitutional bodies had been identified: acts generated by parliaments themselves in the exercise of their legislative activity, acts relating to the area of administrative management, any personal data, documents or acts originating from the administration, and documents received from outside that are already subject to a level of secrecy defined by an external authority. Of these categories, the first is normally public because its outcome must be known. To a certain extent, this also applies to the second category, which is potentially accessible within the limits set by the rules on access to documents. The remaining categories, on the other hand, are subject to confidentiality, which may concern personal situations or situations of national interest. See also Antonio Casu, 'Parlamento e Sicurezza Nazionale.', *Bollettino Di Informazioni Costituzionali e Parlamentari*,



Obviously, the data of interest here is not the implementation of the specific solution, but the relationship with the Perimeter. The interviews revealed that this was an important minimum standard in the definition of security options. It is not known in what way this standard was or was not reflected in the tenders, but they were certainly drafted to introduce specific security requirements, given the sensitivity of the solutions required for the performance of constitutional functions. On the contrary, it can be assumed that it was precisely the specificity of the functions developed that was accompanied by an appropriate security standard, higher than the minimum introduced by the National Security Perimeter.

This is in line with the widespread opinion of the main players in the Italian market. It is no longer possible to continue tendering for the supply of ICT products or services on the basis of the lowest price criterion<sup>662</sup>. For this reason, the new Public Procurement Code includes cybersecurity elements as award criteria<sup>663</sup>. In this respect, there is a marked sensitivity on the part of the Constitutional Bodies, which seek to include security in the requirements of their calls for tender.

As already mentioned, this is not an obligation but a spontaneous adherence to accepted practices. All respondents confirmed the provision of security procedures in accordance with national legislation.

On the one hand, the issue of security incident management comes to the fore. Although there is a positive climate of institutional cooperation between the constitutional bodies and the ACN, the subsequent notification of the CSIRT remains a controversial issue. If cybersecurity is a collaborative effort, failure to notify would not allow for support in activating response procedures, but it is also true that notification could jeopardise sensitive information as it is strictly related to the autonomy of the body. At the time of the interviews, some negotiations on the relationship with the CSIRT and the ACN were still ongoing. It can be assumed that all constitutional bodies now benefit from the wealth of information gathered through incident reporting at national level, but that they are free to decide whether or not to report an incident. In this way, a useful channel of communication has been maintained, limiting side effects. Although there is a certain vagueness in the answers, all the respondents agree that they cannot exclude the existence of situations which, at least in the abstract, would preclude notification for reasons of protecting their constitutional position of autonomy and independence.

On the one hand, the issue of security incident management comes to the fore. Although there is a positive climate of institutional cooperation between the constitutional bodies and the ACN, the subsequent notification of the CSIRT remains a controversial issue. If cybersecurity is a collaborative effort, failure to notify would not allow for support in

---

no. 2 (1994): 131.

<sup>662</sup> COPASIR refers to a statement made by representatives of Telecom Italia concerning the acquisition of products and services by means of a Consip tender. This procedure does not provide for any alternative to the criterion of the highest economic discount. Security requirements are not taken into account in any way. It is precisely in order to compensate for these problems that the legislator intervened to ensure the rapid activation of the CVCN. See Comitato Parlamentare per la Sicurezza della Repubblica, 'RELAZIONE sulle politiche e gli strumenti per la protezione cibernetica e la sicurezza informatica, a tutela dei cittadini, delle istituzioni, delle infrastrutture critiche e delle imprese di interesse strategico nazionale', 21.

<sup>663</sup> The introduction of the vague criteria in Article 108 of Legislative Decree 31 March 2023, n. 36 did not solve all the problems. The recent law 28 June 2024, n. 90 tries to propose a solution. For a more detailed examination, see Cocchi, 'La Cybersicurezza Nel Prisma Del Diritto Dei Contratti Pubblici'; Nannipieri, 'Cybersicurezza e Appalti Pubblici'.

activating response procedures, but it is also true that notification could jeopardise sensitive information as it is strictly related to the autonomy of the body. At the time of the interviews, some negotiations on the relationship with the CSIRT and the ACN were still ongoing. It can be assumed that all the Constitutional Bodies now benefit from the wealth of information gathered through incident reporting at national level, but that they are free to decide whether or not to report an incident. In this way, a useful channel of communication has been maintained, limiting side effects. Although there is a certain vagueness in the answers, all the respondents agree that they cannot exclude the existence of situations which, at least in the abstract, would preclude notification for reasons of protecting their constitutional position of autonomy and independence.

However, it should be noted that some incident reporting procedures were in place prior to the recent implementation of the Perimeter, following the transposition of the first NIS Directive. Some discussions had brought the practice to light, but confirmed its purely optional nature. In this context, the focus was on security, which had already been shown to have a reporting mechanism in place, as opposed to privacy<sup>664</sup>.

In my opinion, the contradictory nature of some of the replies does not call the notification into question. The fact that some institutions denied the existence of this procedure, while others did not, may be due to the different time periods of the interviews. Independently of external relations, the handling of incidents is taken very seriously internally. For example, there is an understanding of the difference between a security event and an incident. Not all events are subject to attention, but there is a defined threshold to trigger alert procedures. This is directly linked to the existence of specific roles for personnel in the event of an incident. Without the need to detail internal procedures, it is sufficient here to recognise an organisation that is focused on response. It is emphasised that mitigation procedures are assigned to experienced personnel. It is not specified whether these are internal or external personnel, but it can be assumed that given the specific training required for these tasks, outsourcing of the service is more likely<sup>665</sup>.

Based on the 15 essential cybersecurity controls for small businesses derived from the CINI, some simple questions were developed to test respondents' readiness on basic issues. These included the provision of access controls and permission minimisation, the existence of anti-malware measures and the use of regular backup practices. Unsurprisingly, there is convergence on these minimum practices, which can be considered common assets for all organisations, both public and private. The usefulness of standards such as ISO 27001 is recognised, but given the small size of their systems, there is no real certification. The standards are used as a benchmark for security self-assessment. Similarly, the Perimeter is seen as a control parameter. The security measures defined in Annex B of DPCM 81 of 2021 are considered as a useful reference standard, although they are not mandatory. Although their applicability is only partial, all respondents recognise the good synthesis achieved by the Perimeter and refer to it when adapting their own security. This process of renewing and adapting security has been underway for some time in each of the responding organisations.

---

<sup>664</sup> This is stated because all respondents denied the existence of a data breach notification procedure. Although the institutions apply the GDPR internally by extension, it is assumed that the data breach procedure, unlike the cybersecurity incident notification procedure, does not add value for these institutions.

<sup>665</sup> Following the President of the Council of the Ministries' directive of 1 August 2015, all public administrations are required to implement a set of minimum ICT security measures. These have become an integral part of the AgID Guidelines.

Progress varied according to the time period of the interviews, but ACN's involvement was always a constant. Since its creation, the Constitutional Bodies have benefited from its support in redesigning their security. In terms of the nature of the support received, most simply referred to the existence of specific agreements, without going into the details of the activities. Among the few details, assistance in carrying out assessments and in drawing up guidelines and internal procedures for security assessment is highlighted.

The whole issue of security measures is directly related to the implementation and operation of the CVCN. Its audit activities are aimed at preventing the procurement of goods and services that could affect security. Regarding the existence of cooperation practices with the CVCN, all respondents gave a rather general answer. The main reason given was the inoperability of the Centre, which only became operational after most of the interviews had been completed and with not a few difficulties. As a result, the discourses on cooperation in the implementation of testing activities were based solely on assumptions of expediency. It can be assumed that the modalities of cooperation with the CVCN were still being defined. Nevertheless, it is possible to make some predictions. As with the rest of the Perimeter Regulations, the results of the CVCN's tests are unlikely to be binding on a competitor's bid. It is more likely that the CVCN's contribution will be indirect in relation to the Constitutional Bodies. The CVCN's technical knowledge, as derived from the previous tests, will feed into the CVCN and may thus become a useful indicator of procurement needs. There will be no support through an actual test phase of deliveries, but technical support will precede and assist in the drafting of the tender in order to exclude a priori potential competitors that could compromise security<sup>666</sup>.

The issue of technical inspections is closely linked to the control powers of the ACN. In the same way that the CVCN will not intervene directly in supplies, or at most at the express request of the constitutional bodies, the ACN cannot carry out inspections or audits of the Constitutional Bodies. This is a natural consequence of the fact that they are not part of the Perimeter. All interviewees agreed that this matter would be specifically addressed in the agreements, which were still being finalised at the time. A verification by ACN may be a useful moment of confrontation, but it remains an interference. It can therefore be assumed, and this was confirmed in the interviews, that the only possible verification can only be the authorised one. In other words, the ACN could be called upon to carry out inspections or audits as part of its security support activities in order to provide feedback on the implementation of security. In any case, any inspection activity will have to follow a request from the Constitutional Body, which will also have to define its limits. The body's staff will at all times monitor the performance of the activities, the results of which must be confidential and cannot have automatic consequences. The identification and implementation of any corrective measures will be at the sole discretion of the body.

---

<sup>666</sup> As a partial complement to what has been said, it should be mentioned that in certain sensitive situations, the Public Procurement Law allows to proceed without prior publication of a contract notice. This is not the place to go into the subject of tendering, but suffice it to say that the constitutional bodies themselves are aware of the possibilities offered by the rules to protect their autonomy and independence. For example, article 55 of the Rules of Administration and Accounting of the Senate of the Republic allows for "the secrecy of tenders or the adoption of special security measures [...] to safeguard the performance of parliamentary functions". On the basis of these possibilities, the Constitutional Court also recently issued a call for tenders, without publication, to equip itself with a server room. See the transparency section of the website of the Constitutional Court.

### V.1.3 The security organisation

This suggests that the Constitutional Bodies themselves are in full control of their own security organisation. This is supported by the fact that the majority of respondents indicated that they use their own staff to manage their ICT assets. Clearly, some services provided by larger organisations also require partial outsourcing of management. Think of all those services that are customised and tailor-made for the performance of the function. In all these cases, it is normal for there to be at least partial outsourcing. However, partial dependence on third parties does not exempt the Constitutional Bodies from having offices in charge of security activities. Although cybersecurity is not an exclusive competence, each of the respondents confirms the existence of both a competent office and a security officer<sup>667</sup>.

Although using different methodologies, all staff surveyed said they had received specific training on cybersecurity risks. Depending on their role, there is specific training to prevent attacks on their credentials and information. The importance of individual awareness becomes crucial to ensure the pursuit of essential functions<sup>668</sup>.

The issue of skills is not confined to personnel, but is also becoming a discriminatory criterion in recruitment processes. Even for non-technical roles, there is a desire to prioritise the recruitment of staff with a greater focus on security issues.

This trend is generally reflected in resource management, although it is not easy to confirm this by reading internal budgets. IT security expenditure is often spread across several budget lines or bundled with other IT equipment expenditure.

In order to gain some insight into the budgets, security-related expenditure was asked to be placed within certain value ranges. With the exception of the smallest constitutional bodies, this expenditure is between 1 and 2 million euro. This is in line with both the growing importance of the issue and the expenditure allocated to IT<sup>669</sup>.

---

<sup>667</sup> Some institutions have a clearly defined internal organisation through various internal rules. For example, the Chamber of Deputies provides for the existence of an IT service and a security service in articles 26 and 32 of its service and staff regulations. While the former is only marginally concerned with security, as it only carries out technological impact analyses, the latter is responsible for performing information security functions. On the one hand, there are internal studies aimed at proposing standards or operational instructions to the Secretary General. In unforeseen and urgent cases, this department can also take the necessary decisions to meet security requirements, directly mobilising the necessary staff. On the other hand, there is also an external liaison activity. Point H refers to [my translation] "relations with police forces and state bodies responsible for security". Clearly, this wording can now be interpreted to include the ACN, and therefore the CVCN and the CSIRT.

<sup>668</sup> Since its establishment, ACN has started to support constitutional bodies by providing them with specific training. As early as the summer of 2022, a summer school was held for central state administrations. The then Minister of Public Administration, Renato Brunetta, had opened the event by stressing the need for action to guarantee training [my translation]: "A country that does not put cybersecurity at the heart of its digital transformation policy is putting its economic prosperity and independence at serious risk". While recalling that €620 million of the PNRR is invested in cybersecurity, a serious skills gap has been reported. See 'Apertura Summer School Cybersicurezza' (Scuola Nazionale dell'Amministrazione, Roma, 12 July 2022), 3, [https://www.funzionepubblica.gov.it/sites/funzionepubblica.gov.it/files/intervento\\_summerschool\\_cybersicurezza\\_0.pdf](https://www.funzionepubblica.gov.it/sites/funzionepubblica.gov.it/files/intervento_summerschool_cybersicurezza_0.pdf).

<sup>669</sup> Taking the example of the Chamber of Deputies and the Senate, it is possible to confirm the increasing allocation of expenditure for IT equipment. If €9,754,175 and €8,962,000 were allocated in 2017 respectively, this will increase to €10,940,000 and €11,190,000 in 2023. These numbers refer to the budget item "Support for administrative processes of digital transformation, collaboration and dematerialisation" in the budget of the Chamber of Deputies and to the item "IT services" in the budget of the Senate.

In order to better identify cybersecurity measures within this otherwise rather broad category of expenditure, respondents were asked to provide examples where possible. On the one hand, it is pointed out that much of the expenditure is derived from professional security services or services that include security features, such as cloud services where the security is managed by the provider. Internally, on the other hand, there are classic security mechanisms. To paint a synthetic picture, measures are in place to protect networks against intrusion attempts, such as the installation of SIEMs to automatically control logs, or partitioning through VPNs. Access is managed centrally through a single user identity control system. All hosts are properly scanned for malware and regularly backed up. In general, it can be said that this is a reflection of those minimum measures whose implementation has become established.

However, there are also interesting measures taken by some organisations in recent years, such as the creation of an internal SOC for the collection and analysis of security events. This demonstrates not only their seriousness, but also their ability to cooperate with the perimeter bodies. The Constitutional Bodies are not passive security actors relying solely on ACN support, but are in some respects demonstrating the development of an autonomous security management capability. Of course, as one can imagine, a serious attack situation would still require support from the rest of the national system, but the complexity of certain interventions should not be overlooked.

In terms of cooperation with the Agency, the funding opportunities opened up by the PNRR are highlighted. Respondents had mentioned the participation of constitutional bodies in several funding calls with proposals aimed at improving their cybersecurity posture. Following the establishment of the ACN, it was tasked with promoting, supporting and coordinating Italian participation in EU and international projects and initiatives, and was therefore designated by the Ministry of Digital Transformation as the implementing body of the PNRR investment 1.5 on cybersecurity. This mandate was followed by several calls for proposals for central administration and Constitutional Bodies<sup>670</sup>. This is further confirmation of the commitment of the constitutional bodies to improving their security.

The table below summarises the amounts awarded in the three calls for proposals.

| Tender Notice | Body                                                  | Intervention                                                                                                                                                                                                 | Funding        |
|---------------|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| 01/2022       | General Secretariat of the Presidency of the Republic | capacity-building in analysis and event detection                                                                                                                                                            | € 1.026.430,16 |
| 01/2022       | Constitutional Court                                  | HW and SW adaptation of the Constitutional Court's server room, acquisition of new services and tools (licences and support services), increase of the Constitutional Court's security against cyber attacks | € 1.041.704,70 |

<sup>670</sup> The reference is to Public Notices 1/2022, 2/2022 and 7/2023. The purpose of the notices was to provide for measures to strengthen and improve the cyber capabilities of constitutional and constitutionally relevant bodies and other central administrations.

|         |                                        |                                                                                          |                   |
|---------|----------------------------------------|------------------------------------------------------------------------------------------|-------------------|
| 01/2022 | Chamber of Deputies                    | modernisation and securing of the internal and external perimeter of the Chamber network | €<br>1.100.000,00 |
| 02/2022 | Senato della Repubblica                |                                                                                          | €<br>405.000,00   |
| 02/2022 | Camera dei Deputati                    |                                                                                          | €<br>230.000,00   |
| 07/2023 | Consiglio Superiore della Magistratura |                                                                                          | €<br>465.000,00   |

The amounts are fully consistent with the answers given in the interviews, taking into account that in addition to the funding, own resources are also allocated.

Although it is not a Constitutional Body, it should be noted that the Superior Council of the Magistracy also received significant funding. This is particularly important after the cyber attack it suffered in April 2023, which led to the complete shutdown of its website<sup>671</sup>. At the time of writing, the security assessment activities, as approved by a resolution of the Presidential Committee of the Superior Council of the Magistracy, are underway. The ACN will assist the Superior Council of Magistracy in the security assessment and, based on the results, will propose appropriate management measures and areas of intervention. All staff will be sensitised<sup>672</sup>.

Although the most relevant security cooperation is with the ACN, other existing relationships were explored. Internally, all respondents confirmed the existence of special tables between the Constitutional Bodies. The construction of the Perimeter and the approach to its participation is an issue that sees constant confrontation between all these particular bodies that seek to coordinate the response to cybersecurity challenges. It is interesting to note that security issues are also being discussed at the European and international level. Each constitutional body has its own representatives in international representative bodies. Although these have no binding role or explicit competence in security matters, cybersecurity is also discussed in these fora. For example, both the Chamber of Deputies and the Senate of the Republic have referred to work in the Inter-Parliamentary Union (IPU) and the European Centre for Parliamentary Research and Documentation (ECPRD). It is not specified whether specific coordination programmes have been carried out or are planned for the security of the IT services that these bodies normally use to carry out their functions. The respondents did not elaborate on the activities carried out at this level<sup>673</sup>.

---

<sup>671</sup> Redazione RHC, 'Attacco informatico al Consiglio Superiore della Magistratura. Attivo il geolocking ma non una soluzione definitiva', il blog della sicurezza informatica, 20 April 2023, <https://www.redhotcyber.com/post/attacco-informatico-alla-consiglio-superiore-della-magistratura/>.

<sup>672</sup> Comitato di Presidenza del Consiglio Superiore della Magistratura, 'ORDINE DEL GIORNO AGGIUNTO - 1265/AC/2023', 6 March 2024, <https://www.csm.it/web/csm-internet/lavori-del-consiglio/dal-plenum?datalink=1709719200000&titololink=seduta+plenum+ordinaria&idAppuntamento=11581#>.

<sup>673</sup> A request was made to the IPU for more detailed information on cybersecurity activities. The response received mainly outlines activities focused on the issue of cybercrime, which, as seen in the paragraph on European policies, is partly intertwined with cybersecurity. The aim is to collect good practices that parliamentarians should implement in their legislation. For example, reference is made to the UN Convention entitled "Creating a safe cyberspace for democracy". See 'Creating a Safe Cyberspace for Democracy', Inter-Parliamentary Union, 24 April 2024, <https://www.ipu.org/event/creating-safe-cyberspace-democracy>. This was also the case for the proper development of legislation against cyber-attacks, which are perceived as a threat to

---

democracy. During the 146th IPU Assembly, a resolution was adopted reaffirming the seriousness of cyber-attacks due to their ability to affect our democracies. The focus is on disinformation attacks, especially during election periods. See '146th Assembly and Related Meetings', Inter-Parliamentary Union, 24 April 2024, <https://www.ipu.org/event/146th-assembly-and-related-meetings>. In this sense, it is clear that cyber-attacks are increasingly perceived as weapons. It is therefore interesting to note that they are dealt with in a parliamentary handbook aimed at promoting and pursuing disarmament. See Inter-Parliamentary Union et al., 'Parliamentary Handbook on Implementation of Securing Our Common Future, the UN Secretary-General's Disarmament Agenda', 2020, 53–58, [https://disarmamenthandbook.org/wp-content/uploads/2021/01/disarmament-handbook-2020\\_v07.pdf](https://disarmamenthandbook.org/wp-content/uploads/2021/01/disarmament-handbook-2020_v07.pdf). As a result, the approach aims to support good cybersecurity legislation rather than the implementation of security by individual parliamentary bodies. This is not surprising, given that the concrete preparation of security is traditionally a national practice and subject to the utmost secrecy.

## VI An ongoing conclusion

The crux of dealing with an issue like cybersecurity is that one has to keep up with the latest developments. There is no time to describe an aspect of it that has been layered by successive interventions. It is therefore always problematic to pull the strings of an evolving subject, because what is written is always tied to the contingencies of the moment.

At the same time, it is somewhat unsatisfactory to try to put an end to a work that will soon require new interventions.

At the level of European policy, security, now understood as cybersecurity, has been reduced to a series of horizontal interventions, given the need to deal with a phenomenon with complex facets.

All the policies outline a change in both the perception and the role of current cybersecurity, from a simple market enabler to a transversal and interconnected priority. Although the market issue is still present as the main reason for implementing security, this must be seen as a façade justification, as the European Union lacks proper powers in the area of security. Many contributions emphasise a change of pace towards a common defence, but only within the limits allowed by the individual member states.

The historical review in chapter II certainly highlights the wide variety of issues that fall under the security umbrella. Even though many of them have not been translated into binding instruments, it is still interesting to try to draw some clusters that can group the European experience to the present moment.

The first can be devoted to all the efforts to standardise security criteria from the 1990s to the recent Cybersecurity Act. This security-focused process has taken place in the context of the broader standardisation process of the entire telecommunications market, but it will spread and influence other regulation as a transversal enabler. Examples include the recent amendment to the eIDAS regulation, which was recently adopted and entered into force in May<sup>674</sup>, or the so-called proposal for a Cyber Resilience Act regulation (CRA), which aims to introduce horizontal cybersecurity requirements for products with digital elements<sup>675</sup>. These and hopefully other European interventions about technology will exploit the certification schemes that will be adopted by the European Commission<sup>676</sup>.

In conjunction with the first group, other groups should be dedicated to more specific

---

<sup>674</sup> European Parliament and Council of the European Union, 'Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 Amending Regulation (EU) No 910/2014 as Regards Establishing the European Digital Identity Framework', Pub. L. No. 1183, UE (2024), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1183>.

<sup>675</sup> The proposal was approved by the European Parliament on 12 March and is currently awaiting formal adoption by the Council before it can enter into force. The original text of the proposal can be found at European Commission, 'Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020 (Cybersecurity Resilience Act)', 2022/0272(COD) § (2022), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0454>.

<sup>676</sup> The first cybersecurity certification scheme was adopted by the European Commission at the beginning of 2024, but many other synergies can be foreseen. In particular, the first Union Rolling Work Programme (URWP) identifies strategic priorities taking into account recent legislative developments. In addition to the CRA and eIDAS 2, the AI Act, the Chip Act, and the new NIS regulation could also be the subject of particular attention. See European Commission, 'COMMISSION STAFF WORKING DOCUMENT - Union Rolling Work Programme for European Cybersecurity Certification', 7 February 2024, <https://ec.europa.eu/newsroom/dae/redirection/document/102292>.



sectors that have taken advantage of the initial security standardisation. The telecommunications sector mentioned above is a perfect example. Various telecommunications packages shaped the current framework until the European Electronic Communications Code intervened to clarify the sector<sup>677</sup>. The same applies to digital identity and authentication services, which, after some initial harmonisation, have been subject to stricter regulation in the eIDAS system.

There are also interventions aimed at defining new institutions, giving them more and more powers and responsibilities for the sake of European integration. The reference is not only to ENISA, whose role has been expanded by the Cybersecurity Act, but also to other expert bodies. While some of these have been created to support the enforcement of specific legislation, others have their own regulation<sup>678</sup>.

To conclude the list of categories from the former first pillar of the European Community, the most relevant and oldest interventions are certainly those on privacy and data protection, on which a vast literature has already been accumulated. Among these, we can also recall some controversial acts, such as the Data Retention Directive, which triggered a long legal saga in front of the European Court of Justice<sup>679</sup>.

However, the most relevant interventions in the internal market are clearly those that explicitly address the concept of resilience, or rather cyber-resilience. Examples are the European legislation on critical infrastructure or the recent amendments to the legislation on network information security. Both pieces of legislation have recently been amended and represent milestones in the European cybersecurity strategy. Not to mention the above-mentioned set of non-binding measures aimed at strengthening the resilience of infrastructure through new investments, research and securing critical supplies<sup>680</sup>.

Although the interventions in the other two former pillars do not have the same impact as those grouped together in this review, they are still worth mentioning. As they are based on weaker EU competences, most of them simply translate into soft regulation or recommendations. Even where enhanced cooperation does take place, the results have to be channelled within each Member State, sometimes with different effects. Binding measures to harmonise criminal law are sporadic.

By contrast, the Union's external action has attracted increasing interest in recent years.

The fallout from the war in Ukraine is destabilising the geopolitical balance in Europe.

---

<sup>677</sup> See paragraph III.1.1 for further details.

<sup>678</sup> Some examples of the former can be found in the new NIS2 Directive, which established the European Cyber Crises Liaison Organisation Network (EU-CyCLONe) to respond to large-scale cybersecurity incidents, or in the new AI Office established in the European Commission under the AI Act. For more details on the NIS system, see section. Not to be forgotten is the European Cybercrime Centre (EC3), which has helped to strengthen cross-border law enforcement coordination. On the contrary, the European Regulation 2021/887 establishing a Cybersecurity Research Competence Centre is a perfect example of the second category of bodies. See Council of the European Union and European Parliament, 'Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 Establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres', 2021 OJ L 13 (2021), <http://data.europa.eu/eli/reg/2021/887/oj/eng>.

<sup>679</sup> Already at this stage, it should be noted that the variety and breadth of data protection topics will be a matter of choice. For content on this topic, see paragraph III.1.2.

<sup>680</sup> The issue of critical infrastructure and NIS will be dealt with extensively in this thesis. See paragraphs III.1.3 and **Error! Reference source not found.** respectively.

Although traditional kinetic actions are still limited to a few well-defined areas, the conflict being waged in the cyber domain has much wider borders and activities are intensifying. Europe's common defence policy has been in motion for several years, with enhanced cooperation, PESCO projects and interoperability standards<sup>681</sup>.

The fundamental problem of the Union's lack of real defence competence remains. The European Union could be called upon to play a key role on the international chessboard in the coming years, provided that it is able to promote its own integration. This is not to undermine all the current efforts, which have seen increasing investment in the development of European capabilities<sup>682</sup>, but simply to point out that research has not yet been matched by a binding common response. Soft, non-binding solutions have always been favoured, leaving the existence of a truly "European" defence beyond the control of individual Member States in the background. This is also reflected in cyber defence cooperation, which remains limited due to the impossibility of introducing real constraints. However much the Member States are encouraged, they remain at the mercy of logics based solely on national decisions.

Although defence is the exclusive responsibility of the Member States, various support and cooperation mechanisms have been developed and introduced in recent years. The European Defence Fund (EDF) has allocated more and more resources to the development of military applications. The most interesting aspect, however, is the diplomatic response to cyber-attacks, which aims to reinforce a common line among member states, outlining a range of possible responses to cyber-attacks. This is yet another demonstration of Europe's ability to create effective rules in the face of complex problems.

All these thematic areas make it possible to correctly frame the interventions of the European legislator and to grasp the breadth of its regulatory policy from the marked regulation to the external action<sup>683</sup>. Although a certain degree of fragmentation between the different policy areas remains, there is hope for a progressive integration of TFEU and CFSP policies<sup>684</sup>.

An interesting prospect for soft integration between the defence and civil sectors for cybersecurity could be the development of reasoned recommendations to bring cyber resilience legislation designed for the market to military use cases. Although defence or criminal investigation and prosecution activities are often excluded from the scope<sup>685</sup>, it would be useful to draw some lines to extrapolate some key contents and logics. This would be in synergy with the important EU funding of military research activities and could

---

<sup>681</sup> These profiles were also recently addressed in a conclusion Council of the European Union, 'Council Conclusions on the EU Policy on Cyber Defence', 22 May 2023, <https://www.consilium.europa.eu/media/64526/st09618-en23.pdf>.

<sup>682</sup> Of course, the European Defence Fund should be mentioned, whose coverage has enabled the development and research of innovative solutions since its creation in 2017. Visit the official website 'European Defence Fund (EDF) - Official Webpage of the European Commission. - European Commission', accessed 9 April 2024, [https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf-official-webpage-european-commission\\_en](https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf-official-webpage-european-commission_en).

<sup>683</sup> These thematic areas are presented in Figure 1 and are also used to group legislative interventions in Table 2.

<sup>684</sup> Daniela Marrani, 'Il Coordinamento Delle Politiche per La "Cybersecurity" Dell'UE Nello Spazio Di Libertà, Sicurezza e Giustizia', *Freedom, Security & Justice: European Legal Studies*, no. 1 (2021): 77–98.

<sup>685</sup> Among the most recent examples, the AI Regulation, finally adopted last June, clearly states that AI systems used for military or national security activities are excluded from its scope. The same applies to any output of AI systems used for the same purposes. See Article 1 of the AI Law.

encourage the overcoming of practices mainly linked to national strategic interests.

Despite the fragmentation just noted, moving from the level of policies to that of European sources makes it possible to highlight some common lines that characterise cybersecurity measures. After overcoming the difficulties posed by the sheer volume of European legislation, it is possible to identify some common and constant practices over the last decades of European regulation.

An incipient of this reasoning can be found in data protection legislation. Without going into the GDPR, the concept of security measures appropriate to the risk could already be found in Article 7 of the former Directive 95/46/EC<sup>686</sup>. As a result, the wording, albeit with different paraphrasing, has been incorporated into various pieces of legislation. The electronic communications sector has also been an ideal vehicle for this, since Directive 97/66/EC and then through the various reforms of the telecoms packages.

As well as talking about adequate security, the reform of the Third Telecoms Package also included the second and essential component of modern internet security, namely the notification of a security incident, known as a data breach in the context of data protection. Strengthened by the GDPR, this practice completes this ideal cycle and brings us back to more recent times.

EU Regulation 2016/679 had refined a risk-based approach, which went hand in hand with the empowerment of the data controller. Institutions such as the prior impact assessment (DPIA) or the concepts of privacy by default and privacy by design are important indicators of this process. On closer inspection, privacy by design and privacy by default refer to a logic that seeks to anticipate the introduction of security measures at a design stage of the solution to be implemented. Above all, however, the essential skeleton of appropriate security measures and notification remains in place, which can be found in Articles 32, 33 and 34 of the GDPR, respectively.

These regulatory instruments highlight the continuity between cybersecurity and data protection. From this perspective, data protection can be placed in synergy with cybersecurity, of which it is not the heir, but the progenitor of its practices<sup>687</sup>. The NIS Directive, when reduced to its essentials, presents the same salient features, to which another typical factor of "doing security" is added. In contrast to the all-encompassing nature of data

---

<sup>686</sup> The relevant text is reproduced here for your convenience: "1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. [...]".

<sup>687</sup> Reference is made here to the relationship between data protection and cybersecurity as synergic, even if it is not a full coincidence [my translation]: "the (public) interest in the security of cyberspace moves in the same direction as the interest (of each individual) in the protection of personal data, insofar as the protection of the environment in which personal data are to be collected, stored, and used is functional to the protection of the right (rights, plural) underlying data protection". See Ponti, 'Il Rapporto Tra Cybersicurezza e Tutela Dei Dati Personali', 2. As the author well analyses, while synergies are possible, conflicting situations can also arise when cybersecurity tools act in violation of fundamental principles governing processing for national security purposes. This is the classic situation of balancing fundamental rights. Several cases have recently been brought before the Court of Justice of the European Union. In addition to Ponti, see the rich analysis of Maurino, "'Cybersecurity', Sicurezza Nazionale e Trattamento Dei Dati Personali'.

protection, which now applies to any processing of personal data relating to a natural person located in the European Union, cybersecurity needs to identify subjects to be brought within its scope. In technical jargon, this is referred to as establishing a security perimeter<sup>688</sup> in one or more relevant areas.

Contrary to what one might think, this logic was not inaugurated by the NIS framework, but has characterised the experience with the identification of critical infrastructures introduced by Directive 2008/114/EC.<sup>689</sup>

While the method is the constant, the values against which the risk is measured, and therefore the actions to be taken, change depending on the regulatory context. For example, while Article 32 of the GDPR focuses on risks to the fundamental rights and freedoms of natural persons, both Article 40 of the European Electronic Communications Code and Article 21 of NIS2 focus on risks to infrastructure. Rights are not always the direct object of protection, but represent a mediated value that benefits from the pursuit of a secure digital system.

The stakeholders are also different. The reference is not only to actors within the scope of the various legislations, but above all to institutional actors<sup>690</sup>. A framework is emerging in which each Member State must be able to rationalise its competences and create structures for effective cooperation.

On the European side, NIS2 certainly inherits these common methodologies from the European resilience system. Not only that, but these features are refined through clearer and more structured procedures. Think of the greater level of detail in the incident notification phase, or the greater clarity in the definition of the scope. At the same time, there is an attempt at better integration<sup>691</sup>, both in terms of European institutional cooperation and the profile of interdependencies between actors<sup>692</sup>.

These ideal foundations have not remained within a dedicated and isolated thematic network, but have spread throughout the successive interventions of the European legislator. The consolidation of an approach based on risk analysis has characterised recent technology regulation in general.

The AI Act<sup>693</sup> is a perfect example of this trend, as it differentiates its obligations on the

---

<sup>688</sup> The identification procedure is described in the complexity of the first NIS paragraph III.2.1.

<sup>689</sup> For a comparison, see paragraph III.1.3.

<sup>690</sup> The Table 2 attempts to map the European regulations with the most relevant national regulations and identifies the reference authority for each.

<sup>691</sup> The Directive will repeal the security provisions (appropriate security measures and notification of security incidents) of the eIDAS Regulation and the telecommunications sector. Stakeholders will be covered by the NIS framework with regard to security. At national level, the national legislator will have to decide whether to designate the old sectoral authorities as NIS authorities, to be maintained in close cooperation with the NIS authorities, or to designate a single authority. The Italian legislator has already partially done this by directly designating ACN as the competent authority in Articles 40 and 41 of the new Electronic Telecommunications Code (Legislative Decree n. 259 of 1 August 2003). See articles 42 and 43 of dir. EU 2022/2555.

<sup>692</sup> The topic of the supply chain remains highly topical. In the new NIS the appropriateness of measures must also be assessed in relation to one's own supply chain. See Article 21 of the NIS2.

<sup>693</sup> On 20 May 2024, Bill 1146 on Artificial Intelligence was introduced. Among the various issues is the question of how to avoid the future use of AI for potential mass surveillance. Given the complexity underlying the regulatory challenges of AI, the idea of creating a dedicated independent agency is gaining ground. Currently, the draft law assigns the regulatory role to ACN and AgID, albeit with a privileged relationship with the Garante Privacy. Please see Laura Ferrari, 'DDL Intelligenza Artificiale: La Società Civile Chiede Più Trasparenza e Tutela

basis of the different levels of risk attributed to AI. Although these are mostly the implementation of requirements specific to the technological object, they also clearly include the prescription of an intrinsic security principle that must characterise the development of AI models<sup>694</sup>. The legal instrumentality of the requirements and procedures introduced by the regulation for the protection of rights is underlined by the introduction of a specific risk assessment for fundamental rights<sup>695</sup>. Also very interesting is the provision for monitoring of AI systems distributed on the market, with notification of incidents caused by high-risk AI solutions<sup>696</sup>.

Cybersecurity is also one of the pillars on which the new eIDAS regulation on digital identity and trust services is based. The symbiotic relationship between trust and security is reflected in the inclusion of cybersecurity requirements using the tools provided by the European Certification Framework of the so-called Cybersecurity Act<sup>697</sup>. Here, too, the issue of incidents returns, because if a trust instrument is compromised, its use must be immediately suspended or revoked so as not to jeopardise the chain of trust<sup>698</sup>.

Returning to cyber resilience legislation, the same principles of risk-based security management and incident notification are clearly evident in the Digital Operational Resilience Act (DORA)<sup>699</sup>. By mandating a layered approach to security, DORA requires institutions to develop comprehensive digital operational resilience frameworks that include preventive, detective and corrective measures tailored to the financial sector's risk landscape<sup>700</sup>. Incident reporting requirements are also built into the framework, requiring financial institutions to notify both national competent authorities and relevant stakeholders of significant incidents within specified timeframes<sup>701</sup>. This is further integrated with testing and continuous monitoring practices. Financial institutions are required to test their operational resilience on a regular basis, in order to assess the robustness of their cybersecurity frameworks<sup>702</sup>.

The European Union has also taken steps to raise the security level of its institutions. They are required to carry out regular assessments, take appropriate measures and draw up a specific plan for their own cybersecurity. The new Cybersecurity Board, which will include representatives from all European institutions, will monitor progress in implementing the Regulation<sup>703</sup>.

---

Dei Diritti', *Agenda Digitale* (blog), 25 September 2024, <https://www.agendadigitale.eu/sicurezza/privacy/ddl-intelligenza-artificiale-la-societa-civile-chiede-piu-trasparenza-e-tutela-dei-diritti/>.

<sup>694</sup> The reference is to Article 15 of the text of EU Regulation 2024/1689, which was finally adopted on 13 June 2024.

<sup>695</sup> See article 27 of reg. EU 2024/1689

<sup>696</sup> See article 73 of reg. EU 2024/1689.

<sup>697</sup> See articles 5c and 12a of the reg. EU 2024/1183 for the security of the identity wallet and articles 19 and 24 for the security of trust services.

<sup>698</sup> See articles 5e and 10 of the reg. EU 2024/1183.

<sup>699</sup> Schneider, 'La Resilienza Operativa Digitale Come Materia Di "Corporate Governance"'; Barbara, 'La "Cybersecurity"'.

<sup>700</sup> See article 15 of the reg. EU 2022/2554.

<sup>701</sup> See article 17-23 of the reg. EU 2022/2554.

<sup>702</sup> See article 24-27 of the reg. EU 2022/2554.

<sup>703</sup> See the text of the Regulation finally adopted last December. See European Parliament and Council of the European Union, 'Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 Laying down Measures for a High Common Level of Cybersecurity at the Institutions, Bodies,

In addition to the capabilities introduced and strengthened by both the NIS and the complementary measures for institutions, the so-called Cyber Solidarity Act, which aims to improve the detection and response capabilities to deal with large-scale cyber threats and attacks, will also intervene in the coming months. The purpose is to set up a European cybersecurity alert system by networking Security Operation Centres (SOCs) across Europe into a European Cyber Shield. The idea behind solidarity is to promote mutual assistance between Member States in the event of a direct attack within the Union. This support will also extend to the post-event debriefing process in order to create a common European incident management culture. To this end, cooperation with the private sector will be used to select a number of trusted operators to form an EU Cybersecurity Reserve that can be deployed at the request of states<sup>704</sup>.

But the best security posture for the Union is not just about strengthening infrastructure and procedures. It is also a market issue for digital products, which should guarantee a minimum level of security before they can be sold. Cybersecurity risks are a horizontal market issue. Without a common standard, there is a risk of destabilising traditional market logics, as each country could define a different level of security to allow certain digital products to enter the market. Manufacturers of digital products will be required to comply with strict cybersecurity obligations and provide ongoing security support throughout the product lifecycle. Conformity assessments will be mandatory to verify that products meet essential cybersecurity requirements, which will be documented in technical documentation and required for CE marking. Post-market surveillance obligations will require manufacturers to monitor for new vulnerabilities, report significant issues to ENISA and ensure timely updates to users. To ensure this uniformity, the final adoption of the Cyber-Resilience Act is expected very soon. It will provide consumers with useful tools to know the security features of interconnected products.<sup>705</sup>

After this review at European level, it is possible to conclude that there is a common practice in the regulatory chaos.

Not only that, but there is also continuity with the measures taken by national legislators. Looking at the National Cybersecurity Perimeter, all the practices mentioned can be found within its implementing components.

On the one hand, D.P.C.M. 131 of 30 July 2020 describes the procedure for defining the perimeter, that is, for identifying the subjects and assets that make up the perimeter and are subject to its obligations. On the other hand, D.P.C.M. 81 of 14 April 2021 defines both the procedures for reporting incidents and the security measures to be taken by the subjects of

---

Offices and Agencies of the Union', Pub. L. No. 2841 (2023), <http://data.europa.eu/eli/reg/2023/2841/oj/eng>.

<sup>704</sup> See the text of the proposal, which is expected to be adopted in April 2024. See European Commission, 'Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Laying down Measures to Strengthen Solidarity and Capacities in the Union to Detect, Prepare for and Respond to Cybersecurity Threats and Incidents', Pub. L. No. 0109, COD (2023), [https://www.europarl.europa.eu/RegData/docs\\_autres\\_institutions/commission\\_europeenne/com/2023/0209/COM\\_COM\(2023\)0209\\_EN.pdf](https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2023/0209/COM_COM(2023)0209_EN.pdf).

<sup>705</sup> See the text of the proposal, which has already been approved by the European Parliament in March 2024. The final adoption of the text is awaiting the agreement of the European Council. See European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cybersecurity Resilience Act).

the Perimeter.

Some might argue that this is not about the influence of European cyber resilience practices, but a more general continuity with international cyber risk management practices that have always characterised risk management systems, from the ISO 27000 family to the NIST framework that led to the birth of our National Cybersecurity Framework.

The objection does not change the fact that this is now a mandatory direction. In a situation of extreme legal complexity, operators cannot be left with uncertainty as to its application. Even if this is an authorisation, the mere reference to "security measures appropriate to the risk", without at least a broad indication, is totally unsatisfactory, especially in view of the jagged landscape of small and medium-sized enterprises that characterises Italy.

Despite the undeniable complexity resulting from the tangled web of secondary legislation, the national legislator's attempt to define the perimeter was undoubtedly laudable, as it aimed to provide greater clarity for the actors identified. In view of the regulatory complexity that characterises the sector, some scholars are starting to talk about the existence of a broader "cybersecurity legal field", in order to outline the convergence and tensions between the various regulatory networks, which are increasingly interdependent<sup>706</sup>. Initiatives such as ERACLITO, which has been mentioned several times, will increasingly support ACN and the various institutional players in the coming years. The legislator should keep the door open to the possibilities of synergy between university bodies, start-ups and public administration by providing the tools for such cooperation.

Meanwhile, the national legislator is already grappling with the next challenges posed by this magmatic regulatory scenario.

The establishment of the Perimeter and the creation of the ACN have streamlined the national infrastructure by definitively dividing the three core cybersecurity functions (cyber intelligence, cyber defence and cyber resilience) into distinct areas. Initially, there was some overlap between intelligence and cyber resilience, but these functions have since been clearly separated<sup>707</sup>, although the ACN still carries out national security responsibilities<sup>708</sup>. New interventions have already taken place, and many more will take place in the near future<sup>709</sup>.

Law n. 90 of 28 June 2024 made a first adjustment to the system. One of the most striking innovations is undoubtedly the "virtual" extension of the National Security Perimeter, through the extension of the obligation to notify incidents to a large part of the public administration, or the possibility of voluntary notification<sup>710</sup>. On this occasion, the legislator begins to prepare the plan for the subsequent transposition of the NIS2 directive, aligning the

---

<sup>706</sup> Comandè and Casarosa, 'Aspettando La NIS2 ["Network and Information Systems"]', 52.

<sup>707</sup> Except for the residual possibility left by Decree-Law 82 of 2021 for the President of the Council of Ministers to assign the residual non-exclusive functions in cyber matters to the delegated authority under Article 3 of Law 124 of 2007.

<sup>708</sup> This approach is common to other countries, such as the United States, which have opted for the specialisation of agencies dealing with national security. See Renzi, 'La Sicurezza Cibernetica', 546.

<sup>709</sup> As a partial complement to what has been written, reference is made to the start of the legislative transposition process of NIS2. The draft legislative decree for transposition has started the approval process in the Chamber of Deputies. See legislative decree scheme of 17 June 2024, n. 164.

<sup>710</sup> See Article 1 of the law 28 June 2024, n. 90. The article is accompanied by an increase in penalties for repeated failure to comply with the obligation to report incidents.

notification deadlines for the subjects of the Perimeter with those of the directive<sup>711</sup>.

In a synergetic manner, ACN's control powers will be strengthened with the possibility of sending timely notifications on the exposure of particular vulnerabilities to all relevant actors in the Italian cybersecurity sphere<sup>712</sup>, who will have to resolve them within 15 days. Moreover, the important addition of ACN's power to classify the information received on incidents should not go unnoticed<sup>713</sup>.

As the legislator has already intervened to improve the coordination relationship between the ACN and the judiciary<sup>714</sup>, reference is made to the activities of the intelligence services. In particular, it introduces the possibility of postponing certain cyber resilience activities if this is necessary for the pursuit of intelligence activities<sup>715</sup>.

Still on the subject of public administration, all public entities referred to in the law under review will have to appoint a cybersecurity contact person to implement a cybersecurity plan and carry out continuous monitoring, also taking into account possible vulnerabilities in the implementation of encryption<sup>716</sup>. This person will be the point of contact for all ACN business<sup>717</sup>.

---

<sup>711</sup> Casarosa, 'L'armonizzazione Degli Obblighi Di Notifica'.

<sup>712</sup> The obligation may be addressed to NIS entities, telecommunications entities or Perimeter entities. See Article 2 of the law 28 June 2024, n. 90.

<sup>713</sup> Certainly, this provision does not solve every problem, but it at least helps to highlight a problem, which is certainly in contrast to the progressive expansion of the service. Information about vulnerabilities in a computer system is normally classified at least at the national RESTRICTED level. This level of classification already has important management implications, requiring the use of appropriate encryption in appropriately segregated environments. The question that remains in the background is whether, and under what conditions, those involved in incident notification are required to classify the information before sending the report. On the other hand, the rule introduced by the law could be read as an exception to the reporting party's obligation to classify. See Article 4 of the law 28 June 2024, n. 90.

<sup>714</sup> The reference is to the introduction of paragraph 4-bis to article 17 of Legislative Decree 82 of 2021, which obliges the ACN to forward crime reports under article 371-bis to the National Anti-Mafia Prosecutor. See Decree law 10 August 2023, n. 105 as amended by law 9 October 2023, n. 137.

<sup>715</sup> See Article 6 of the law 28 June 2024, n. 90. Intelligence activities can conflict with the need for transparency and the exchange of information on security incidents. If the ACN is normally required to provide the National Anti-Mafia and Anti-Terrorism Prosecutor with information relevant to the exercise of its functions, the President of the Council of Ministers could order the postponement of information obligations or resilience activities. Although this measure must be strictly necessary for the institutional purposes of the Intelligence System for the Security of the Republic, it would be desirable to introduce a maximum time limit for deferral, at least for mandatory information to COPASIR. Not to mention that everything will depend on the actual interpretation that each President of the Council of Ministers will give to the strict necessity, since there is no counterweight that could prevent him from exercising this prerogative. Strengthening the role of the President of the Council of Ministers in his cybersecurity powers should not lead to the marginalisation of the role of Parliament. This had already been observed by the doctrine at the beginning of the construction of the Perimeter. See Carotti, 'Sicurezza Cibernetica e Stato-Nazione', 639.

<sup>716</sup> The law requires that all cryptographic measures in use follow ACN and privacy authority guidelines to avoid known vulnerabilities. A National Encryption Centre will be established at ACN to oversee cryptographic standards and research. See Articles 9-10 of the law 28 June 2024, n. 90.

<sup>717</sup> See Article 8 of the law 28 June 2024, n. 90. As positive as the identification of a contact person is, it does not seem that the legislator has really taken into account the views expressed during the hearing. Such a figure would have benefited from a greater impact on administrative processes, given the cross-cutting nature of cybersecurity in relation to administrative digital services. See Erik Longo, 'Audizione Informale per Il Disegno Di Legge in Materia Di "Disposizioni in Materia Di Rafforzamento Della Cybersicurezza Nazionale e Di Reati Informatici"' (AC 1717). Camera Dei Deputati, Commissioni Riunite I e II - Roma, 28 Marzo 2024', *Rivista Italiana*



Equally important, ACN will be tasked with defining the concept of 'cybersecurity elements' that can be used as award criteria in public tenders<sup>718</sup>.

After this update about the current state of the legislation in Italy, it is possible to draw a conclusion by referring to the experience of constitutional bodies.

To summarise what emerged from the interviews, the security of the central organs of the State is in a transitional situation. Although the security Perimeter reflects the desire not to impose the automatic inclusion of the Constitutional Bodies, with all the consequences in terms of compliance, there is positive cooperation on their part. Despite the slowness that has characterised the activation of the ACN and its entire support system, which is not yet fully operational, there is a strong focus on security issues. A path of accompaniment and, one could say, alignment with the Perimeter, which has been welcomed as a tool to increase its level of protection, has begun immediately.

However, the optional nature of its provisions has led to many of its practices being adopted and transferred to the technological level, from security measures to incident reporting. Of course, the question of how to combine autonomy and independence with security remains. All cooperation and exchange of information with ACN must always be seen in the light of this objective. Should the two values come into conflict, it is conceivable that the balance would tip towards protecting the position of autonomy and independence of these particular state bodies. Cybersecurity tools must not become a channel for the executive to interfere in the reserved sphere of other powers. Consequently, security checks by ACN should only be carried out upon request and in a manner agreed with the Constitutional Bodies.

The choice of the Constitutional Bodies to align with the security rules and practices of the Perimeter framework is a choice in the realm of their Constitutional autonomy. This demonstrates a conscious exercise of their self-governing powers, and not a mere submission to external standards. Under these conditions, it is possible to hope for the continuation of a virtuous collaboration, capable of combining delicate constitutional needs with the security of digital infrastructures, which inevitably become an extension of the State.

Furthermore, this choice can be explained by the fact that, in the renovation of their security systems, it is easier for the Constitutional Bodies to adopt an outlined structure like the Perimeter, rather than creating an entirely new one. In cybersecurity, adopting well-established standards and common practices facilitates this process. There would be, in any case, an important continuity, as these frameworks are widely recognized and applied across various sectors. Confronting the lack of specific literature on this particular issue, it should be emphasized that this is a personal and humble interpretation, offered as a reasoned hypothesis.

With regard to the initial research hypothesis, it can be concluded that the Perimeter has reached a good level of involvement of constitutional bodies, both in terms of technological support and economic resources. There is no evidence of a potential conflict between security and the autonomy and independence that characterise these bodies.

In fact, the transition highlights a significant specialisation in the security approaches of these Constitutional Bodies, moving from mere physical protection to digital security of their

---

*Di Informatica e Diritto*, no. 1 (2024): 4.

<sup>718</sup> See Article 14 of the law 28 June 2024, n. 90. The concept of cybersecurity elements was first defined by Article 108 of the new Public Procurement Code (Legislative Decree No 36 of 31 March 2023).

systems. This evolution reflects the broader modernisation of state institutions, where the integrity of digital infrastructure is now paramount.

## I Appendix I - Compliance for the Perimeter Subjects

This appendix reports some results of the ERACLITO research project. This research has been developed within the research group of the University of Genoa and represents the first part of a process to reconstruct the compliance requirements for Perimeter subjects. Although the annexes to D.P.C.M. 81 already propose a series of measures to be implemented, the focus is limited to a number of security measures. As the D.P.C.M.s instead highlight a broader process for compliance, the purpose of this paper is to reconstruct this process in measurable terms. Both strictly technological and organisational or procedural requirements should be covered at the end of the regulatory research.

As anticipated, the following result represents a step ahead of what is required by the project.

The Table 1 in paragraph I.6 of appendix I is based on an article-by-article reading of all the implementing D.P.C.M.s of the Perimeter and attempts to extract a set of functional requirements that can be used as measurable indicators of compliance of the Perimeter subjects.

The table is divided into several columns. Starting from the left, the first column shows the article and the reference paragraph. The second column summarises the requirement arising from the standard. The third column indicates the addressee of the requirement, who is responsible for its implementation. The fourth column attempts to describe the requirement in a comprehensive manner to provide an aid to understanding. Where the requirement involves an exchange of information, the fifth column indicates the recipient of the information. The sixth and final column attempts to provide a checklist of controls to assist in verifying the implementation of the requirement, where this is appropriate.

The table is up to date with respect to the Perimeter DPCMs and presents the main updates up to spring 2024.

The next steps in the research will attempt to map these functional requirements to existing standards such as the National Cybersecurity Framework, NIST 2.0 or ISO 27001. The table is preceded by an introduction that examines how an international standard works. The paragraphs I.1, I.2, I.3, I.4, and I.5 of appendix I provide a general overview of how the technical standard works. The main ISO standards for cybersecurity are recalled and the ISO 27001 family is used to introduce the basic operation of a risk management system. The review continues with an introduction to the NIST standard, which was updated in February this year with the release of version 2.0. Some figures and discussions focus on the categories of the previous NIST, but this does not affect the purpose of the description. The discussion closes with the Italian National Cybersecurity Framework, which is used as a reference by D.P.C.M. 81 and which was developed by CINI and La Sapienza University of Rome on the American NIST model.

Since the target audience is not necessarily large companies or central public administrations that have dedicated internal functions for cyber risk management, the aim of this review is to provide the essential outlines of this process.

### I.1 Some basic concepts about standards and guidelines

Dealing with issues that encroach on the technical sphere consequently entails a review of the main concepts. Reference has often been made to the logic of risk, in relation to the identification and adoption of the most suitable technical and organisational measures to mitigate it. The underlying balancing operation goes completely outside the legal sphere,

distancing itself from any relationship with rights, which are reduced to a mere component of the equation. The objective is to identify the best balance between prevention and cost to pursue the implementation of those controls that are the most effective.

Deferring the details to the following discussion, it should simply be noted that this matrix pertains to a well-established tradition at the international level, which is not limited solely to the management of IT security and the risks associated with it. Risk can be intrinsic to a wide variety of activities, and therefore different families of technical standards deal with regulating it in different sectors.

Without any claim to completeness on a subject, which would require adequate space for a full examination, an attempt will now be made to reconstruct the essential regulations governing technical standardisation. The opportunity will be taken to clarify some common terminologies and to briefly explain some operating methodologies.

For these purposes, it may be useful to briefly recall the European legislation regulating standardisation. The first interventions in this field were already in the late 1980s. Focusing on the relevant sources, one can therefore refer to those first European interventions for technical standardisation in the field of information technology and telecommunications<sup>719</sup>.

Clearly, these must be placed in the context of a broader international relationship. The global reach of technology, especially in the ICT sector, has always been matched by a shared international production aimed at ensuring the interoperability of systems. For this reason, the interventions of the European or national legislator or, more generally, of any authority at local level, do not play a leading role, but are concerned with filling any gaps. This is mainly due to the complexity, the need for the rapid publication of new standards and the economic importance behind the adoption of effective standards. Nevertheless, the essential starting point is regulation at the international level, which must be appropriately transposed to the regional level. European standardisation authorities are only required to take supplementary action where minimum accuracy is needed for information exchange or interoperability.

“Where an international standard, draft international standard or international technical specification in telecommunications offers clear provisions allowing its uniform application [...] these provisions will be adopted unaltered in the European standard, European prestandard, or telecommunication functional specification [...]. Only where such clear provisions do not exist in the international standard, [...] the European standard, European prestandard, or telecommunication functional specification will be written to clarify or, where necessary, supplement the international standard<sup>720</sup>.

Having said this, it is possible to outline how the standardisation process follows a top-down movement, where the steps leading up to the national level must be those that are strictly necessary. The ultimate goal is to ensure maximum sharing and interoperability, aspects that have always characterised technological development, particularly in the ICT sphere.

A decade later, attempts to facilitate the circulation of information around technical regulations and standards would be added to ensure greater awareness among operators and regulators<sup>721</sup>.

---

<sup>719</sup> ‘87/95/EEC: Council Decision of 22 December 1986 on Standardization in the Field of Information Technology and Telecommunications’, 036 OJ L § (1986), <http://data.europa.eu/eli/dec/1987/95/oj/eng>.

<sup>720</sup> See article 2 of the Council decision 87/95/EEC.

<sup>721</sup> ‘Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 Laying down a

The reason for this is to minimise the impact on the economy and the common market, as the introduction of national requirements for a product could affect the free movement of goods. It is therefore essential that the Commission always has the necessary information before adopting technical rules. At the same time, all Member States should exchange information on their national draft technical regulations. Potential barriers to trade resulting from technical regulations should only be allowed where they are necessary to meet essential requirements or public interest objectives. In short, an attempt has been made to imbue the European standardisation system with the indispensable principles of transparency, openness and, above all, consensus between the different states. As further confirmation of this, the only exception to the principle of notification of new technical standardisation projects is when they are merely a transposition of an existing European or international standard.

The final point concerns funding. Over time, the standardisation sector has required increasing investment to follow and accompany technological evolution. This is why the European Union realised the need to contribute to the financing of European standardisation in view of its future usefulness in supporting its legislation<sup>722</sup>. This entire system is currently being replaced to meet the need to adapt to the latest developments and future challenges of European standardisation.

The stratification of amendments had affected the readability of the normative texts, which were therefore codified<sup>723</sup>.

Having established the current regulatory basis, it is now necessary to recall some key concepts to introduce how technical standardisation works. Firstly, the concept of standard, for which the regulations provide a definition, must be clarified. "'Standard' means a technical specification, adopted by a recognised standardisation body, for repeated or continuous application, with which compliance is not compulsory"<sup>724</sup>.

It is precisely the non-binding character of standards that represents the most significant difference to a mandatory norm. The scope of standardisation is not based on 'an imposition from above', but on mutual recognition, i.e. on the convenience of carrying out a given activity

---

Procedure for the Provision of Information in the Field of Technical Standards and Regulations', 204 OJ L § (1998), <http://data.europa.eu/eli/dir/1998/34/oj/eng>.

<sup>722</sup> 'Decision No 1673/2006/EC of the European Parliament and of the Council of 24 October 2006 on the Financing of European Standardisation', 315 OJ L § (2006), <http://data.europa.eu/eli/dec/2006/1673/oj/eng>.

<sup>723</sup> 'Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European Standardisation, Amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and Repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council Text with EEA Relevance', 316 OJ L § (2012), <http://data.europa.eu/eli/reg/2012/1025/oj/eng>.

<sup>724</sup> See Article 2(1) of Regulation (EU) 1025/2012. Due to the different translations of the text of the regulation, a further clarification of terminology is necessary. In the English version, which is reproduced here, the definition uses the term "standard". In other translations, such as the Italian one, the concept is translated with the term 'standard' technique. As a result, an ambiguity is created due to the attribution of a more specific meaning to the term 'standard', contrary to the general meaning of the English version. The English word 'standard' has been transposed into Italian to indicate the product of the application of a 'norm'. It should be emphasised that there is not necessarily a biunivocal relationship between the two concepts. A 'norm' may be associated with several 'standards', but it is also true that a 'standard' may not necessarily derive from a 'norm'. In terms of content, the 'norm' sets general requirements, whereas a 'standard' defines technical characteristics for the purpose of interoperability. Having closed this parenthesis, from now on the terms will be used respecting the meanings attributed by the English version.

in the same structured manner<sup>725</sup>. This is the only incentive for organisations to conform to a standard, compliance with which can be certified through an audit<sup>726</sup> by an accreditation authority. Obtaining certification is synonymous with competitiveness, because it is a reliable means of demonstrating to one's stakeholders one's ability to meet certain requirements within a given sector.

A second aspect to be considered is the existence of standardisation bodies at different levels, from international to national<sup>727</sup>.

---

<sup>725</sup> It should be pointed out that complying with a standard entails the implementation of various controls, which may partially overlap with controls made mandatory by a mandatory regulation. In other words, there is a fruitful exchange between standards and mandatory regulations. On the one hand, the legislator in regulating a certain sector, characterised by a high level of technicality, may prescribe the adoption of controls partly covered by a standard. On the other hand, during the development of standards, great consideration is given to the existing standardisation, which is usually mapped against the controls to be introduced. The result of these two movements, respectively from technical regulation to mandatory regulation and vice versa, is an approximation of the two levels that find a natural alignment with each other. Simplifying further, the more the existing legislation introduces certain requirements, the more the standards will seek to promote compliance by including specific controls that take account of the new changes in the legislation.

<sup>726</sup> An audit is a formal procedure for verifying the information and documentation of an organisation or individual, in this case concerning information security policies. The objective is to express an opinion on the accuracy of the information on the one hand, and on the other hand on its correspondence with applicable standards and regulations. An audit consequently involves a subject that examines and a subject that is examined. Depending on the relationship between the two, there may be different types of audits. One speaks of an internal or external audit depending on whether the audit is carried out by personnel of the organisation itself or by an independent third party, respectively. An internal audit is also referred to as a first-party audit, while an external audit is referred to as a third-party audit. There is also an intermediate case between the two, which is a second-party audit, which occurs when the audit is performed by a customer of the product or service provided. Usually this happens in order to verify the reliability and compliance of the supplier. For more information see Rajkumar Banoth, Narsimha Gugulothu, and Aruna Kranthi Godishala, *A Comprehensive Guide to Information Security Management and Audit*, First edition (Boca Raton: CRC Press, 2023), chap. 2.

<sup>727</sup> The continuation of the same definition identifies four types of standards depending on the level on which the standardisation body adopts it. In that order, a standard may be international, European, harmonised, or national. A harmonised standard is also a standard at the European level. Let us now give a few examples of standardisation bodies. At the international level are the International Organisation for Standardisation (ISO), the International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU). At European level, there are the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications Standards Institute (ETSI), as clearly referred to in Annex I of Regulation (EU) 1025/2012. Finally, at national level, the *Ente Nazionale Italiano di Unificazione* (UNI) can be mentioned. Each member state is obliged to notify the European Commission of the standardisation bodies at national level.

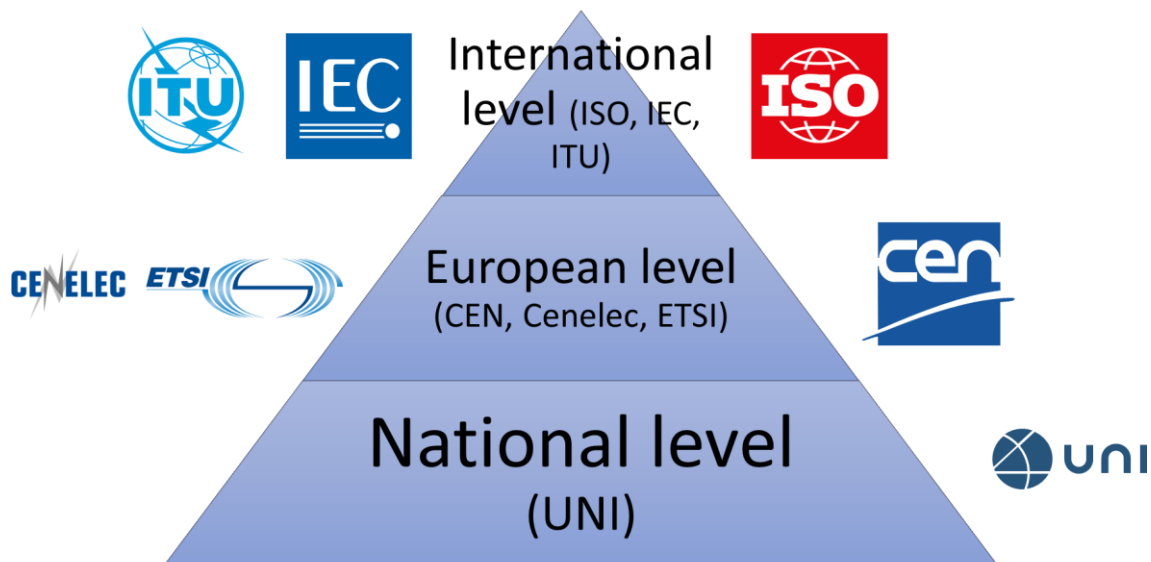


Figure 25 - Standardisation Bodies

To conclude the review of definitions, another frequently used terminology is that of a technical specification, i.e. "a document that prescribes technical requirements to be fulfilled by a product, process, service or system"<sup>728</sup>. At the same time, it has become common to refer to the concept of guidelines or good practices. These represent the consolidation of an optimal balance between the identification of reliable parameters and flexibility in application. They may have elements of similarity to standards in some respects, but usually differ in the greater level of detail in the description of the procedures and controls to be implemented. Furthermore, while conformity to a standard can be certified, conformity to a guideline is not equivalent to certification<sup>729</sup>.

So far, we have talked about de jure standards, because they are approved by recognised technical standards bodies. Since there are many other relevant actors in the technical sphere, it is clear that technical production is not only the domain of a small circle of recognised actors. Although this is not the place to go into this in depth, it should at least be emphasised here how the 'official' technical production is flanked by an 'unofficial' one, because it results from a consolidated and customary use by sector experts<sup>730</sup>.

Consequently, the involvement of civil society and experts in the field is an indispensable element in the adoption of a technical standard, the main steps of which are summarised in Figure 26.

<sup>728</sup> See Article 2(4) of Regulation (EU) 1025/2012.

<sup>729</sup> In many cases, a guideline will accompany a standard to support its implementation. A well-known example is the famous ISO family of standards dedicated to information security, ISO 27000. The ISO 27001 standard is accompanied by the ISO 27002 guideline. It is sometimes oversimplified to say that it is possible to certify compliance with the guideline. Although the guideline certainly helps in the correct implementation of the standard, certification can only exist based on the guideline.

<sup>730</sup> An example of a technical standard produced by a private stakeholder in the field of cybersecurity is the Transport Layer Security (TLS) protocol. The TLS protocol is designed to secure communications over computer networks, particularly the Internet. It provides encryption, authentication, and message integrity to ensure the secure transmission of data between applications and services. The TLS protocol was developed by the Internet Engineering Task Force (IETF), a private, non-profit organisation made up of volunteers from a variety of companies, universities, and research institutions. The IETF is responsible for developing Internet standards, including protocols such as TLS, through a collaborative and consensus-based process.

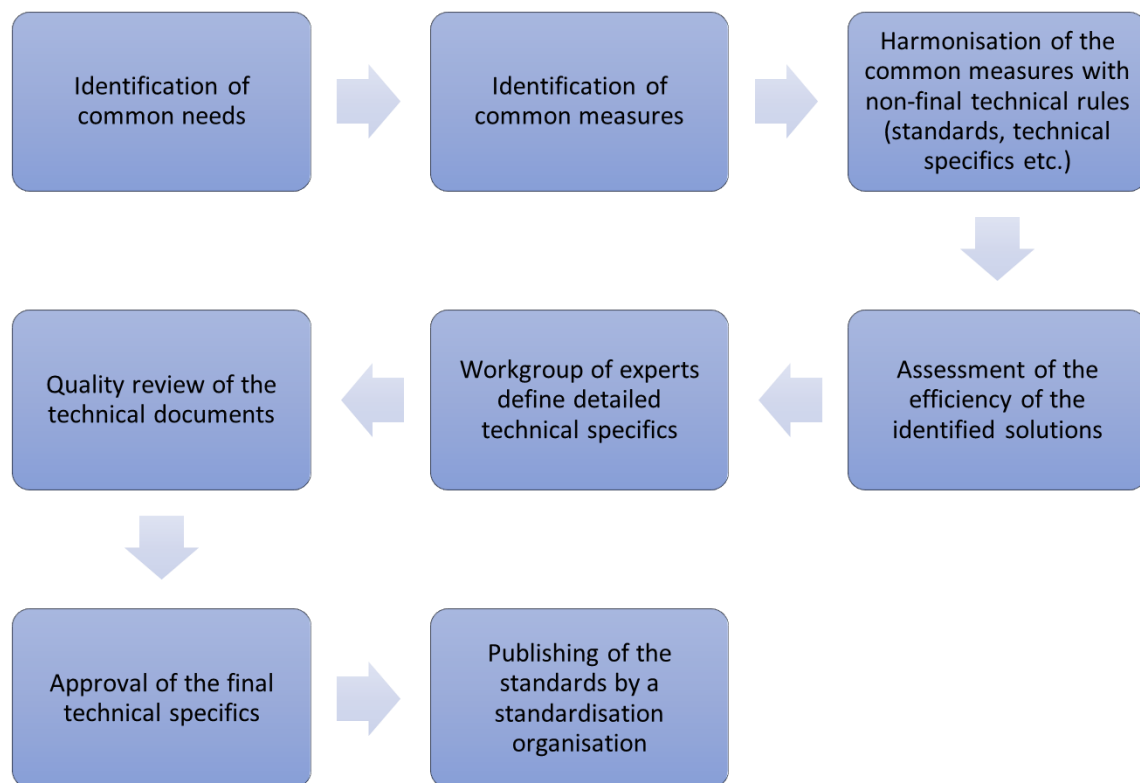


Figure 26 - Standardisation common procedure

First, there is an informal identification of measures to address a common problem. This initial moment is then followed by several steps of consolidation, first through informal standards and then through more detailed production. There is usually input from working groups of experts before the standard is finally approved by the standards bodies. The final result is a standard containing one or more detailed technical specifications. The publication is usually accompanied by an acronym representing the abbreviation of the standardisation body<sup>731</sup>.

## I.2 What is a management system: an example from ISO 27001

To conclude this high-level introduction, and without claiming to be exhaustive, let us consider what is the key to interpreting the meaning of technical production. Given the non-binding nature of this type of source, any standard or guideline can be thought of as a tool available to all those entities, at various levels, that are faced with security problems. It is not only a question of compliance, i.e. meeting the requirements imposed by general and sectoral regulations, but also of setting up an effective risk prevention system against any impact on

<sup>731</sup> For example, the famous ISO/IEC 27001:2022 takes the abbreviation of the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC). This is followed by a numerical code which, on the one hand, refers to the family of standards and, on the other, identifies the specific standard within it. The 27000 family refers to information security management, while the numbers up to the hundreds refer to the specific standard. In this case, the most important standard for information security, cybersecurity and privacy is recalled. The number after the colon represents the version, by indicating the year. There may also be several abbreviations relating to standardisation bodies. This indicates that the technical documentation has been implemented by one or more standards bodies at regional level. For example, ISO 27002:2013, the companion guideline to ISO 27001, has been transposed by the European standardisation body (EN ISO/IEC 27002:2017) and then by the various national bodies (UNI EN ISO/IEC 27002:2017).



information security. In technical terms, this means setting up a management system that can be adapted to the characteristics of each entity, be it a company or a public administration. The ultimate goal is to achieve an optimal level of risk, i.e. the best balance between the resources used and the performance sought. Since this balance must always be measured against a very specific subjective situation, there is no "one size fits all" solution, but rather a better solution depending on the size, sector, available resources, and objectives to be pursued. In addition to the complexity that arises from the heterogeneity of the issues, there is also the complexity that arises from the wide variety of methodologies. Not only can the same methodology be applied in very different ways depending on the subject, but several different methodologies can be chosen<sup>732</sup>. Not to mention that larger players prefer to create bespoke methodologies to better suit their needs.

Despite their differences, all frameworks share some basic characteristics. In particular, the structure is extremely similar and can be schematised by the stages of the Deming Cycle<sup>733</sup>.

---

<sup>732</sup> The best known and perhaps the oldest management system is that of ISO 9001, concerning quality management, first published in 1987 by the International Organisation for Standardisation. It was in turn based on BS 5750 from the British Standards Institution, which had proposed the standard to ISO in 1979. Prior to that year, several similar standards had been used for quality management and customer satisfaction, but without any attempt at uniformity. In the cyber field, on the other hand, there is the aforementioned ISO 27000 family and other examples from other organisations. For example, the NIST Cybersecurity Framework, developed by the American organisation of the same name, and COBIT (Control Objectives for Information and Related Technologies), developed by ISACA.

<sup>733</sup> Dr. W. Edwards Deming, a remarkable statistician and management consultant, invented the Deming Cycle, also known as the PDCA Cycle. This quality management method emphasises the importance of continuous improvement of processes and structures and provides companies with a structured and logical framework for achieving and maintaining high quality standards. Into motion the operation goes with the prompt of the 'Plan' stage, where established targets and objectives, devised tactics, and constructed operation schemes can be located. Implementation of the schemes takes place during the "Do" stage, and data is compiled to determine results. During the "Check" stage the evaluations of outcomes are analysed and compared to the initial goals. Finally, the "Act" stage commences as adjustments are made based on data collected and analysed with the enhancement of performance in mind. For further information see W. Edwards Deming, *Out of the Crisis* (The MIT Press, 2018), <https://doi.org/10.7551/mitpress/11457.001.0001>; Domenico Lepore, *Deming and Goldratt : The Theory of Constraints and the System of Profound Knowledge : The Decalogue* (Great Barrington, MA : North River Press, 1999), <http://archive.org/details/deminggoldrattth0000lepo>; Peter B. Petersen, 'Total Quality Management and the Deming Approach to Quality Management', *Journal of Management History* 5, no. 8 (1 January 1999): 468–88, <https://doi.org/10.1108/13552529910290520>.

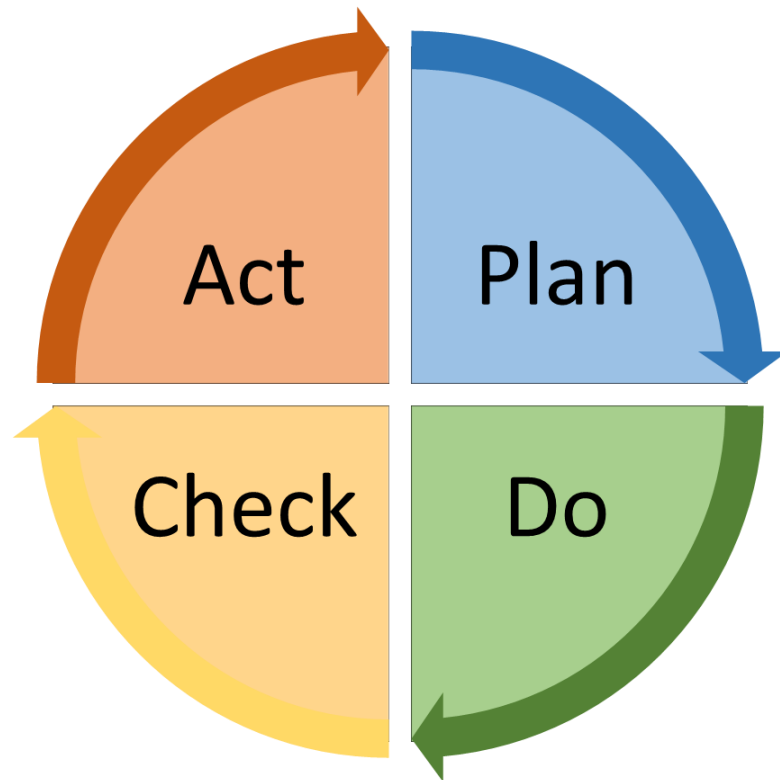


Figure 27 - Deming Cycle

This reminder is important because it allows us to understand some of its basic principles. On the one hand, the application of a framework is a dynamic endeavour, which can be photographed at a given moment, but which must be able to maintain a continuous adaptation with respect to changes external to the organisation. On the other hand, it is important to emphasise the breadth and diversity of the aspects covered by the different stages of the framework. The four-stage division that results from the Deming cycle shown above can be further described by the sequence of chapters that originally represented the structure of ISO 9001. The effectiveness of these procedures was such that they were later transferred to the structure of other management systems in the ISO family. To understand the complexity that characterises its processes, we will now proceed to identify its main steps. In doing so, we will enter the field of information security management by following the steps of ISO 27001<sup>734</sup>.

---

<sup>734</sup> The ISO 27000 family of standards, maintained by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC), has historical roots dating back to the mid-1990s. Its immediate predecessor is British Standard Institution Standard 7799, published in 1995. The text was written by the then government's Department of Trade and Industry (DTI) and was later revised and adopted by international standards organisations. The first part was first translated into ISO/IEC 17799 in 2000, which went through a revision process in 2007 to become ISO/IEC 27002. The second part has instead been incorporated into ISO/IEC 27001.

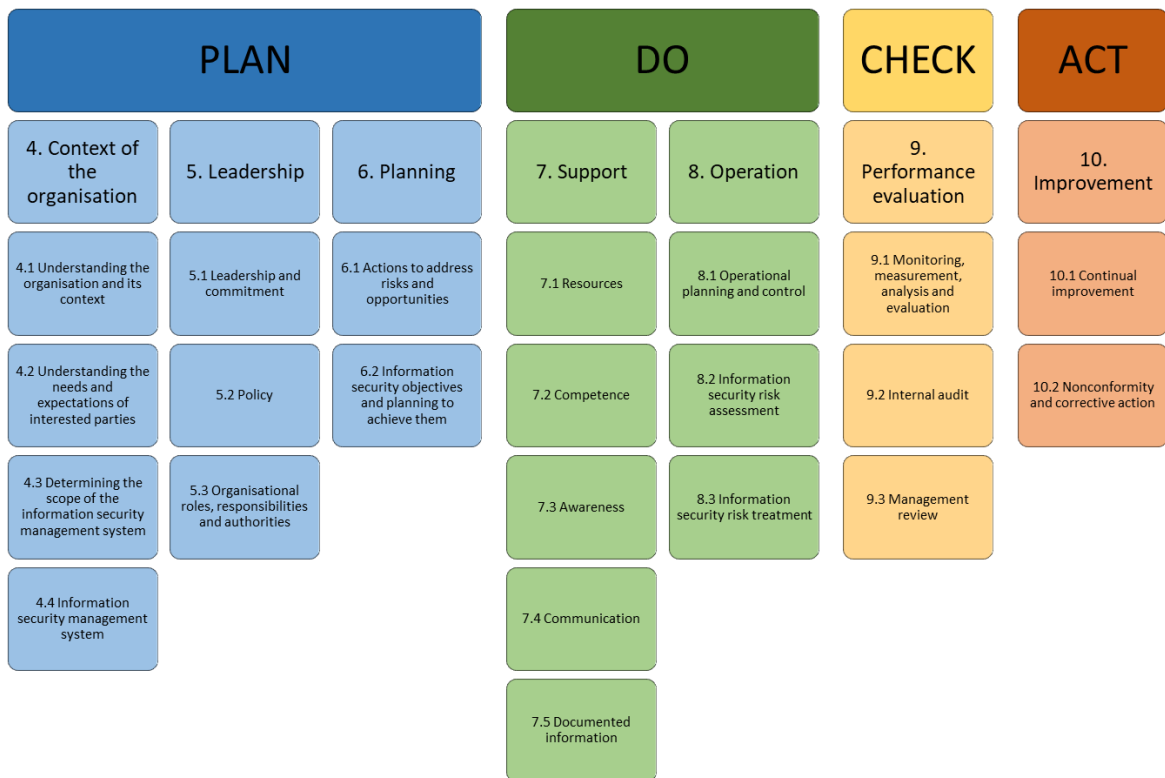


Figure 28 - ISO 27001 through the stages of the Deming Cycle

Figure 28 is the result of overlaying the stages of the Deming Cycle with the chapters and sections that normally make up the structure of an ISO.

Following this well-established methodological order, an essential commentary can be made, taking into account the introductory purpose of these arguments. Although with some differences due to the national context, the same logic underlies the procedures of the National Cybersecurity Framework<sup>735</sup>.

The first step in implementation consists of a careful study of the context in which the organisation operates. Since the aim of the standards is to be able to adapt to the needs of any entity, regardless of its characteristics, an initial contextualisation effort is necessary. In fact, the indications that can be derived are at a high level and identify the requirements, but not the recipes for their implementation, which must be defined on a case-by-case basis.

Contextual analysis is therefore an essential component. The sector or size of the organisation may give rise to internal and external factors relevant to the provision of security.

Internally, the organisation needs to assess its resources, internal processes, organisational structure and approach to information management. Externally, different threat scenarios and different regulatory requirements will need to be reflected in the organisation.

However, the security that all these factors contribute to is not absolute security, but the best possible security, considering the pursuit of the organisation's objectives. This is an important aspect to consider. In the case of a business activity, there is a balance to be struck with the exercise of private autonomy. The latter certainly cannot take precedence over

<sup>735</sup> The following paragraphs will be devoted to the perimeter and its regulations.

security, but neither can it be totally compressed, i.e. negated. This is even more the case when these considerations are made by public subjects who represent collective interests. From this point of view, security is a value that must play a supporting role without becoming an end in itself. It is always a question of finding the right balance, also to satisfy the interests of those stakeholders that revolve around the same entity. These stakeholders may be investors, suppliers or, more simply, end users or citizens. The expectations of all these stakeholders must be considered as strategic priorities to be pursued and regularly updated<sup>736</sup>.

Once the objectives and the factors that may affect them are clear, the correct scope of the information management system needs to be identified. It is normal for such a system not to cover all corporate assets, but to pursue well-defined objectives in line with those of the organisation. Some examples of defining the scope of the system may be the company's branches, its departments, its staffing plan, or the type of information or the purposes pursued by certain assets. This selection is the result of a series of logical steps, the first of which is certainly the identification of the information needed to pursue the objectives. The next step is to identify the resources and processes involved in managing this information. The result is the maximum coverage of the system, which, in summary, must include not only the information, but also all those elements that prepare for its proper management. This is useful to maximise the result and avoid wasting resources by concentrating efforts only where necessary. Given the heterogeneous structure of each organisation, close cooperation between different functions and levels is required, with the involvement and input of the relevant stakeholders.

Above all, a strong commitment from the top is required. The board of directors must regard security as a priority and demonstrate this by issuing clear policies that enshrine this

---

<sup>736</sup> The issue of security balance is much debated. On the one hand, it must be balanced with other organisational values. The issue of security balance is much debated. On the one hand, it must be balanced with other organisational values. See Olive Emil Wetter, 'From Short-Term Goals to Organizational Objectives : Managing Security Control Using Goal Setting' (University of Zurich, 2012), <https://doi.org/10.5167/UZH-164118>; Janne Merete Hagen, Eirik Albrechtsen, and Jan Hovden, 'Implementation and Effectiveness of Organizational Information Security Measures', *Information Management & Computer Security* 16, no. 4 (10 October 2008): 377–97, <https://doi.org/10.1108/09685220810908796>; Sushma Mishra, 'Organizational Objectives for Information Security Governance: A Value Focused Assessment', *Information & Computer Security* 23, no. 2 (8 June 2015): 122–44, <https://doi.org/10.1108/ICS-02-2014-0016>. On the other hand, it is inherent in the influence of public values on private decisions. A perfect example is the recent European attempt to regulate large technological platforms through the so-called Digital Market Act. See Erik Longo, "'Digital Services Act' - Libertà Di Informazione. Libertà Di Informazione e Lotta Alla Disinformazione Nel "Digital Services Act"', *Giornale Di Diritto Amministrativo*, no. 6 (2023): 737–45; Andrea Simoncini, 'La Co-Regolazione Delle Piattaforme Digitali', *Rivista Trimestrale Di Diritto Pubblico*, no. 4 (2022): 1031–49; Gianluca Buttarelli, 'La Regolazione Delle Piattaforme Digitali: Il Ruolo Delle Istituzioni Pubbliche', *Giornale Di Diritto Amministrativo*, no. 1 (2023): 116–27; Laura Ammannati, 'Regolatori e Supervisorì Nell'era Digitale: Ripensare La Regolazione', *Giurisprudenza Costituzionale*, no. 3 (2023): 1453–73; Carlo Colapietro, 'Libera Manifestazione Del Pensiero, Fake News e Privacy, Oggi', *Dirittifondamentali.It*, no. 2 (2022): 422–38. The topic was also discussed during the seminar "Cybersecurity, A.I. and principle of legality: a constitutional perspective", Genoa, 10 April, 2024. The speakers also discuss the potential for using the "ordering of the algorithm" as a way to regulate the behavior of platforms. They suggest that by understanding and shaping the way that algorithms structure and organize information, it may be possible to promote more democratic and equitable outcomes. However, they also acknowledge that this approach raises complex technical and ethical questions, and that it is not a substitute for more comprehensive regulation of platforms. Overall, the conference highlights the need for a more nuanced and multifaceted approach to the regulation of platforms, one that takes into account the complex and dynamic nature of these systems and the diverse impacts they have on society.

position<sup>737</sup>. It follows that adequate resources must be allocated, also in terms of personnel, since roles and responsibilities must be assigned to individuals with the appropriate skills<sup>738</sup>. Finally, the tasks to be performed must be publicised to ensure awareness by all levels of the organisation.

Once all the requirements have been defined in terms of the organisation's objectives, roles and responsibilities, the actual planning phase begins. The starting point is a risk management process, a phase common to the operation of several standards. The idea of optimal planning is to define the best relationship between the actions to be taken and the resulting mitigation. For a better understanding, it is useful to refer to ISO 27005, which details all the stages of the risk management process, as shown in Figure 29.

---

<sup>737</sup> The very definition of policy contained in ISO refers precisely to this: "intentions and direction of an organisation, as formally expressed by its top management".

<sup>738</sup> The definition of the most appropriate roles for each organisation in terms of information security has undergone a process of standardisation over time. Consequently, several classification frameworks now exist to analyse the figures to be introduced in the organisational chart. In particular, the roles are accompanied by a mapping of the necessary skills, greatly simplifying both the training and recruitment process. "Today, cybersecurity professionals continue to contend with challenges that have built since the outbreak of COVID, while also facing the consequences of greater economic pressure across the globe". However, the gap between the needed workers and the available workers continues to grow. See ISC2, 'ISC2 Cybersecurity Workforce Study 2023', 2023, 3–4, [https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2\\_Cybersecurity\\_Workforce\\_Study\\_2023.pdf?rev=52055d08ca644293bd7497725bb7fcb4](https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=52055d08ca644293bd7497725bb7fcb4). Among the various reference frameworks, those developed by the most renowned certification institutes such as the EC-Council and SANS must certainly be mentioned. For an extremely precise classification, reference should be made. To the so-called NICE framework of NIST, which provides an in-depth explanation of each individual role and assigns the skills required to fulfil it. See Rodney Petersen et al., 'Workforce Framework for Cybersecurity (NICE Framework)' (National Institute of Standards and Technology, 16 November 2020), <https://doi.org/10.6028/NIST.SP.800-181r1>.

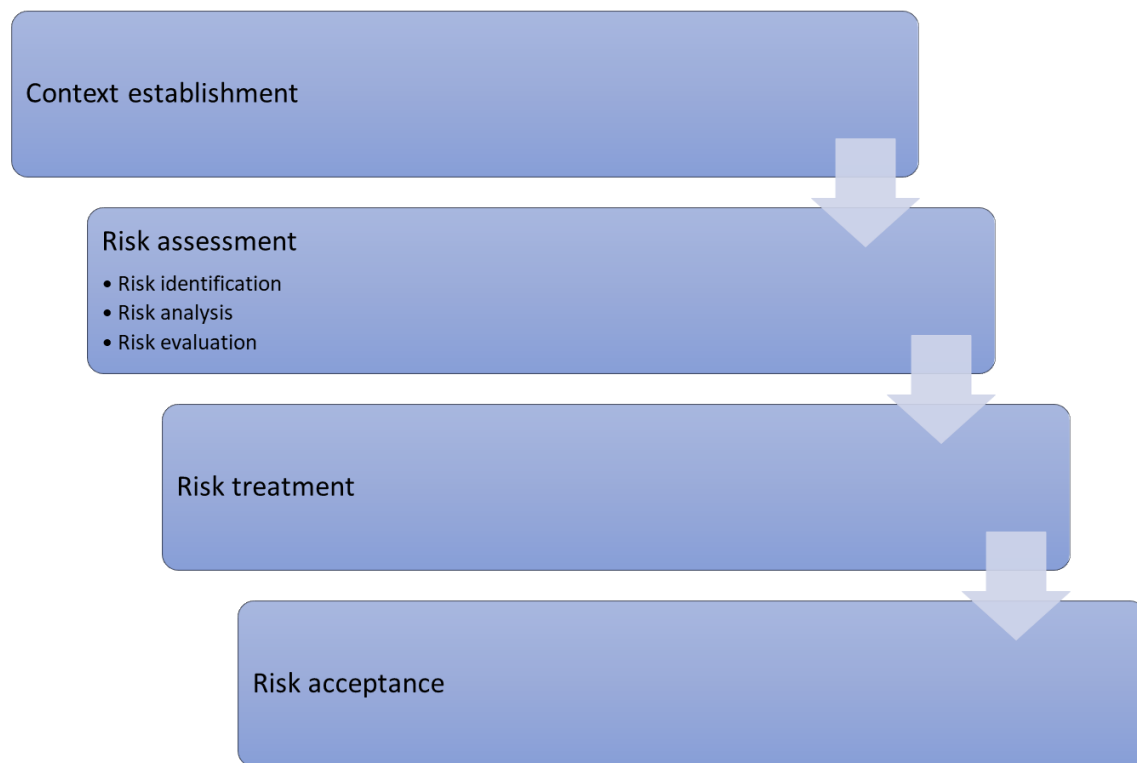


Figure 29 - Risk Management process

Just like ISO 27001, this process cannot be carried out in absolute and abstract terms, but always requires continuity with respect to the organisational context.

Before proceeding, however, it is appropriate to introduce some specific terminology that will be used. The following definitions can be found in both ISO 27001 and 27005, although the same concepts may apply to a wider range of situations.

For example, up to this point we have often referred to an organisation in general terms. However correct it may be to refer to the idea of a legal entity, this can sometimes be limiting as it may simply be a person or group of people united by a common purpose<sup>739</sup>. It is precisely the objectives that are a central theme because they make it possible to explain the concept of risk, which is defined as the effect of uncertainty on objectives<sup>740</sup>.

Various external events, the occurrence of which is uncertain, could affect objectives and prevent their pursuit. It is more correct to speak of the probability of occurrence, one of the two characteristics that define an event. The other characteristic is that of consequences, which defines the impact of the occurrence of an event on objectives. This is why risk is usually calculated as the product of the impact of an event and its probability of occurrence. From this perspective, it is easy to see why objectives are an indispensable parameter for calculating risk, which cannot be assessed in the abstract. Of course, not all events have a negative impact, since the term "event" is used in a neutral way. Within this set, it is possible to identify, in the first place, those events that are relevant from an information security point of view<sup>741</sup>. Among the latter, those that have a negative impact are commonly defined as

---

<sup>739</sup> The definition of "organisation" is: "a person or group of people who have their own functions with responsibilities, powers and relationships to achieve their objectives".

<sup>740</sup> The definition of risk is: "effect of uncertainty on objectives".

<sup>741</sup> The following is the definition of "event": "identified occurrence of a system, service or network state that indicates a possible violation of the information security policy or a failure of controls, or a previously unknown

computer incidents<sup>742</sup>, which may be the result of a computer attack<sup>743</sup>. In general, this is a possible example of a threat<sup>744</sup>. The other side of the coin is vulnerability, which is a weakness in an asset that can be exploited by a threat<sup>745</sup>.

Since the purpose of risk management is to control risk and thereby reduce it, appropriate controls are identified to be implemented within the organisation. These can be understood as measures capable of modifying the risk by acting on its components, i.e. the impact or probability of occurrence<sup>746</sup>.

As controls are the result of choices made by a particular organisation, they are not necessarily mandatory. Consequently, a control is not necessarily an obligation, but rather a requirement. The search for an optimal balance involves the identification of an objective in terms of the controls to be implemented. Now that the tools for effective understanding of the subject have been provided, it is possible to briefly analyse the individual steps shown in the diagram. Apart from the contextualisation phase, which coincides with the identification of the organisation's objectives, the heart of the risk management activity lies in the risk assessment phase. This is divided into three basic moments. The first is risk identification, which consists of identifying all the threats that could lead to the materialisation of various risk scenarios. By predicting these scenarios, the risks that could affect the organisation are derived and monitored in terms of existing vulnerabilities. Although there are now well-established methodologies and mappings for the identification of threat scenarios<sup>747</sup>, they are always the result of a mental exercise. In other words, no matter how much reference is made to the best shared experience, there will always be unforeseen risks because they have

---

situation that may be security relevant".

<sup>742</sup> The following is the definition of "computer incident": "a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security".

<sup>743</sup> The following is the definition "computer attack": "an attempt to destroy, expose, alter, disable, steal or gain unauthorised access to or use of an asset".

<sup>744</sup> The following is the definition of "threat": "potential cause of an unwanted incident that may result in damage to a system or organisation".

<sup>745</sup> The following is the definition of "vulnerability": "a weakness in an asset or control that can be exploited by one or more threats"

<sup>746</sup> Consider, for example, the risk associated with a ransomware attack on a military network. If it contained national security information, it is easy to imagine that the impact of such an attack would be high, rendering the entire content of the network unavailable. On the one hand, control through regular backups could almost completely mitigate the risk by acting on its impact component. On the other hand, isolating the network would achieve the same result, but by acting on its probability of occurrence.

<sup>747</sup> ISO 27005 itself has an annex listing the main risks (Annex C), or ENISA periodically publishes a report containing a taxonomy of the risks identified at European level. This taxonomy takes the form of a mapping contained in a spreadsheet and should not be confused with the usual threat landscape. The latter is a broader report that aims to capture trends and is less analytical. See 'Threat Taxonomy', File, ENISA, accessed 13 November 2023, <https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view>; 'Enisa Threat Landscape 2022', Threat Landscape (European Union Agency for Cybersecurity, November 2022), <https://data.europa.eu/doi/10.2824/324797>. For scenario construction, the OpenFAIR standard is commonly used, which has the advantage of establishing a precise and measurable use of terms. A scenario is simply a statement composed of several factors. The structure is reproducible based on this sentence: '[Threat actor] affects the [effect] of [asset] via (optional) [method]'. For more on this topic, see 'How to Write Strong Risk Scenarios and Statements', ISACA, accessed 12 November 2023, <https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-31/how-to-write-strong-risk-scenarios-and-statements>.

never happened before.

Assuming that there is an inherent margin of error in risk identification, the final product is a risk register<sup>748</sup>. Each risk must be correctly assigned to a responsible person and its magnitude correctly quantified.

Without going into the details of risk calculation systems, which would require a more extensive study, it is sufficient here to recall the distinction between qualitative calculation systems, quantitative calculation systems and so-called semi-quantitative systems<sup>749</sup>. Regardless of the type of approach adopted, the methodology must be comprehensible and repeatable, both in terms of procedures and results. In addition, the available resources and time must be considered. The result of this step can ideally be represented by a Cartesian plane, as shown below.

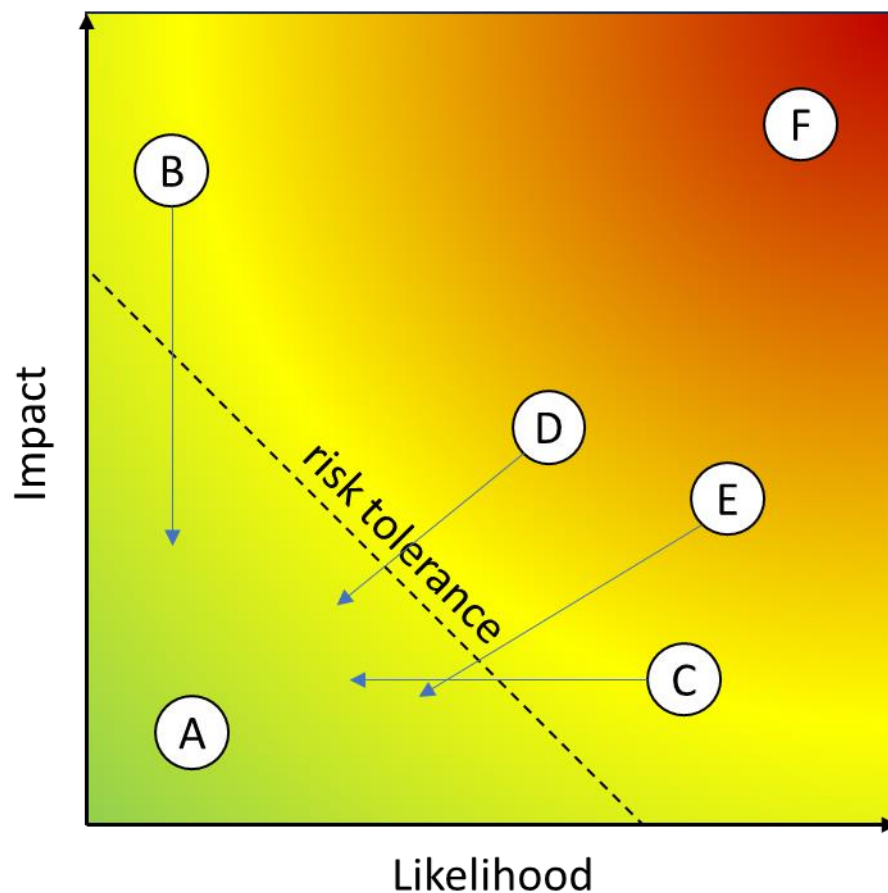


Figure 30 - Risk assessment process

All the risks identified have been analysed and their magnitude quantified using the

---

<sup>748</sup> There are several templates that serve as an aid to the correct annotation of risks and their classification. ISACA's is widely used and provides an initial mapping for assessment activities.

<sup>749</sup> Quantitative risk calculation methods use numerical data and mathematical models to accurately assess risk. An example is the FAIR (Factor Analysis of Information Risk) methodology. Qualitative methods, on the other hand, are based on experience and expert judgement and provide a subjective assessment of risk. Typically, this category of methods makes extensive use of interviews with employees. An example of this category is the CRAMM (CCTA Risk Analysis and Management Method) developed by the UK government agency CCTA (Central Computer and Telecommunications Agency). Finally, semi-quantitative methodologies combine qualitative and quantitative elements for a more precise risk assessment.



calculation methods adopted. Since the characteristics of each risk are the severity of its consequences, expressed as impact, and the probability of its occurrence, the position of the circles on the plan explains this relationship.

The next step is to identify the risk tolerance threshold for the organisation. Not all identified risks necessarily require action, as acting may be more costly than accepting the impact. The aim is not to eliminate the risk, but to bring it within an acceptable threshold. The dotted line in Figure 30 aims to identify this optimal balance and where it is appropriate to take corrective action. The final phase is the actual risk management phase. As mentioned earlier, interventions act on risk components by reducing them. Ideally, the optimal reduction should be sufficient to bring the risk within the tolerance threshold.

For the sake of completeness, it should be emphasised that not all possible options for risk treatment involve risk reduction. As shown in Figure 30, only some of the identified risks are actually managed. Those marked with an arrow are mitigated by two main methods. The first and most familiar is the implementation of countermeasures and security controls to reduce the impact or frequency (C, E and D). The implementation of controls is described in detail in ISO 27002, which classifies them according to different characteristics and categories<sup>750</sup>.

The second method, on the other hand, is to transfer the risk by concluding an insurance contract or outsourcing the activity (B). In this way, the impact perceived by the organisation is reduced because it is absorbed by another party. Obviously, this strategy is only viable where the frequency of occurrence is low.

Then there are the cases where it does not pay to manage risk, which lie at the two opposite ends of the Cartesian plane. The first (A) is easy to understand because the risk is already within tolerance. In this case, it would be more costly to implement countermeasures, if possible, than the consequence of the risk occurring. These situations, where the risk is simply accepted, occur at the end of the risk management process, where the resulting risk is considered a 'residual risk'.

Conversely, the excessive impact and the high probability of occurrence lead one to question not so much the adoption of countermeasures, but rather the performance of the activities involving the identified risk. Since the benefits of the activity would not cover the costs, it is better to avoid the risk altogether. This is why many risky but socially beneficial activities are sometimes carried out at a loss because they are in areas of market failure.

The methodology described above is divided between the planning and implementation phases. To return to the diagram, the picture needs to be completed with the provision of appropriate supporting resources, including staff, technology, infrastructure, and adequate spending capacity. Note how special attention is also paid to the skills profile, so that the staff identified can perform their tasks effectively. Not only that, but everyone needs to be made aware of security risks. The role of effective communication, both internally and externally, is also emphasised. This is an important aspect to emphasise for the purposes of certification, which requires documentation of the procedures and controls in place.

After the implementation phase, the circle begins to close with the effectiveness review phase, which is based on the continuous monitoring of processes. This is not only an evaluation based on indicators, but can also take more structured forms, such as internal

---

<sup>750</sup> The classification adopted covers several different perspectives. For example, the type of control, i.e. whether it is applied before (preventive), during (detective) or after the incident (corrective), or the cybersecurity asset to be protected. For a more detailed review, see ISO 27002.

audits. The audit procedure consists of a systematic and documented verification of the compliance of the information management system. Based on the results, it is possible to assess a revision of the system according to a logic of continuous improvement. The final phase consists of the implementation of these improvements, focusing on the non-conformities found.

### I.3 Other ISOs related to information security

Before concluding this international overview, it should be emphasised that ISO 27001 and 27002 are not the only standards in the field of cybersecurity. Within the family of ISO 27000, dedicated to information security management, there are several other standards that are commonly adopted. Figure 31 identifies some of the ISO building blocks that are fundamental components of a proper cybersecurity posture.

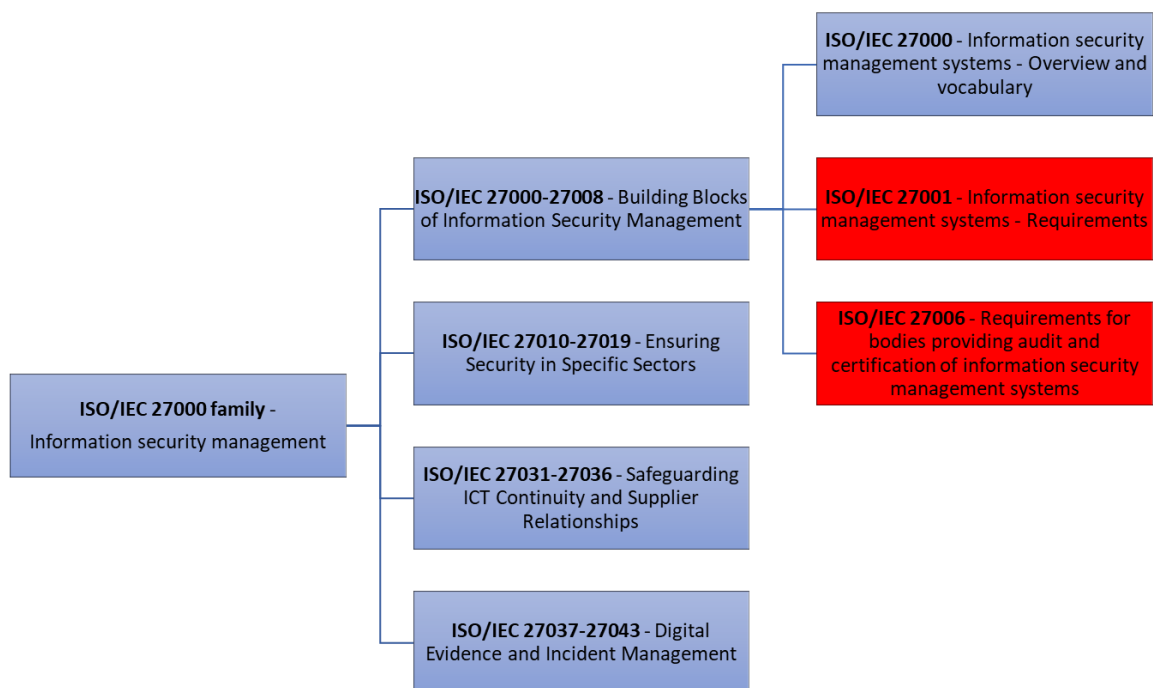


Figure 31 - ISO 27000 family

The proposed classification is not intended to be rigid, but to serve as a useful conceptual framework in order not to get lost in the analysis. The aim is to broaden the scope of the analysis, without going into detail, and to provide an insight into the complexity of the aspects covered by standardisation.

The first block, which has already been partially addressed in the previous section, comprises those aspects that are fundamental to the regulation of information security. Because of their particular importance, some of these have been highlighted in Figure 31. Not only ISO 27000, which provides the basis for a common vocabulary, but above all ISO 27001 and 27006, which lay down the requirements for the certification of one's own information security system on the one hand, and for the certification of auditors on the other. These are the few existing standards in the industry for obtaining certification, accompanied by a set of general guidelines to support and enable best practice implementation. Figure 32 shows a more detailed exploded view of this part, showing in red those standards and in green those guidelines for which a replacement text is being developed.

As standards are intended to apply to the widest possible range of issues, the requirements focus on prescribing objectives. From a compliance perspective, these can be understood as 'what' to do, leaving the definition of 'how' to individual organisations, which remain free to choose different approaches. The guidelines that accompany these standards help to identify the best methods of implementation.

In this respect, both ISO 27002 and ISO 27005 play a key role in the integration of an information management system, as already described. ISO 27002 covers best practices for the implementation of security controls that an organisation might choose to implement. Its Appendix A contains an exhaustive list of controls, each accompanied by a practical implementation guide and classification. ISO 27005 specifies practices for managing risk, from its identification to its treatment, providing a systematic and reproducible approach. These tools prepare the way for choosing the best security controls. Undoubtedly, ISO 27001 involves the selection of controls and risk management. The implementation of these controls, once selected, and the management of risk in practice are aspects provided by these two guidelines.

In addition to ISO 27001, ISO 27003 and 27004 address other aspects of building an information management system. The former focuses on the integration methodology to best fit the management system to the organisation. This is a great help in overcoming the vagueness that often characterises the requirements, which leave a lot of room for manoeuvre. At the same time, there is a strong link between standards and guidelines. Sometimes there may be an autonomy between the two, but those mentioned are a perfect example of an aid to meeting requirements. In particular, ISO 27003 allows you to identify areas where you are lacking and to take action.

The next ISO, 27004, is ideally the next step. Once the management system has been implemented, its effectiveness needs to be assessed with a view to continuous improvement. The two ISOs are then in a cyclical relationship, as the results of the improvement phase lead back to planning and implementation, and therefore to ISO 27003. Among the various tools that can be used for this purpose is the audit, which can be carried out internally or by a third party, impartial organisation. Such bodies are often certified to carry out information security audits. They are certified based on ISO 27006, which sets out the requirements for accreditation and covers several aspects to ensure the competence, impartiality and independence of the auditors. Particular emphasis is also placed on the audit process and the certification of the decision. Effective implementation is ensured by ISO 27007, which provides guidelines for conducting both internal and external audits.

The approach is based on that of ISO 19011, which is the general standard for auditing management systems. In general, guidance is given on the audit programme, the personnel to be included in the audit team, the process, and the preparation of the final report. Regarding the audit process, guidance is provided on how to check compliance with the requirements. Specifically on these aspects, ISO 27008 focuses on how to verify the correct implementation of security controls. It then proposes a procedure for selecting the control to be verified, the testing methodology and the evaluation of the results. Figure 32 summarises the ISOs mentioned above.

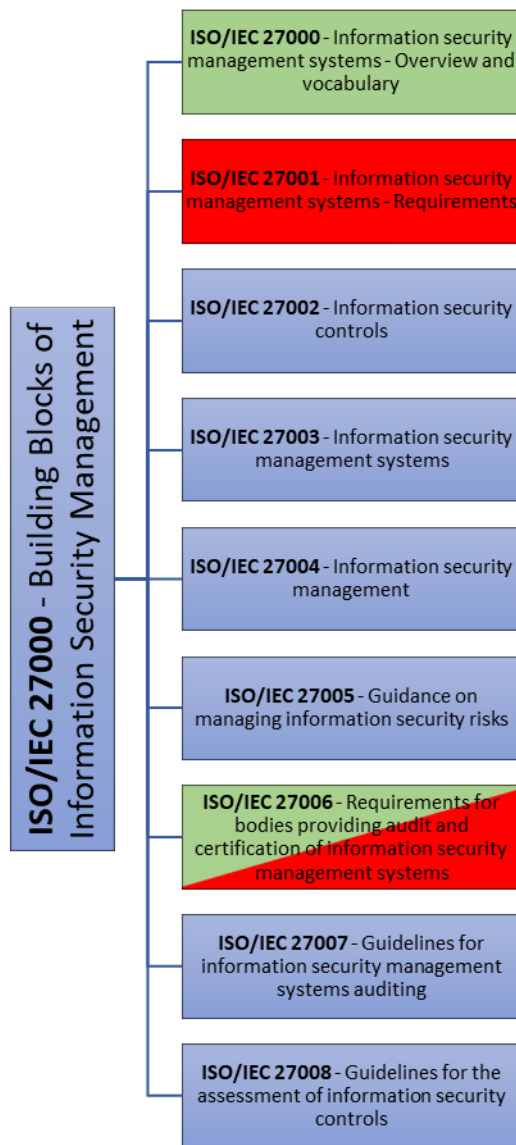


Figure 32 - ISO 27000 family - Information Security Management

While these can be seen as the main building blocks for the most effective implementation of ISO 27001, there are other guidelines that complement other detailed aspects. The first, addressed by ISO 27010, is that of cross-sector or cross-organisational communication. As the number of cross-sector relationships increases, organisations operating within them may need to develop communication systems. This is often critical to improving performance in the pursuit of common goals, as any information exchange must address security issues. Next, ISO 27013 addresses an issue that is often mentioned when dealing with security, namely the trade-off with quality. Often an organisation will want to implement its information management system in line with a quality control system. The result is the need to find the best compromise between the two conflicting objectives.

No less important is the issue of governance, because any system of rules, including those relating to information security, must provide for a group of people with the authority and responsibility to enforce security policies and procedures. As mentioned above, this is a complex process because it requires a balance with the organisation's objectives. In this respect, ISO 27014 provides useful guidance on both the management of personnel and the overall structure of the framework.

Finally, there is the management of the economic impact of security decisions, an issue addressed by ISO 27016. In order to make informed decisions, it is necessary to be able to measure the impact on the bottom line. Risk management needs to meet economic objectives as far as possible.

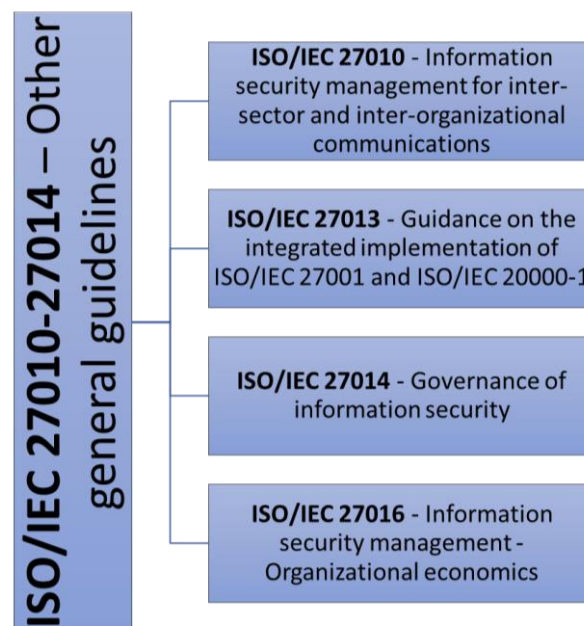


Figure 33 - ISO 27000 family - Other general guidelines

Following that hypothetical ladder represented by Figure 34, the second block is dedicated to sector-specific measures. Particular attention has been paid to the telecommunications sector, the financial sector, the cloud, especially where personal data is processed, and the power generation sector. Given the level of detail and the need to reflect a narrower scope, all these ISOs are being revised and replaced (green colour) or have already been withdrawn following the outcome of the periodic evaluation (grey colour).

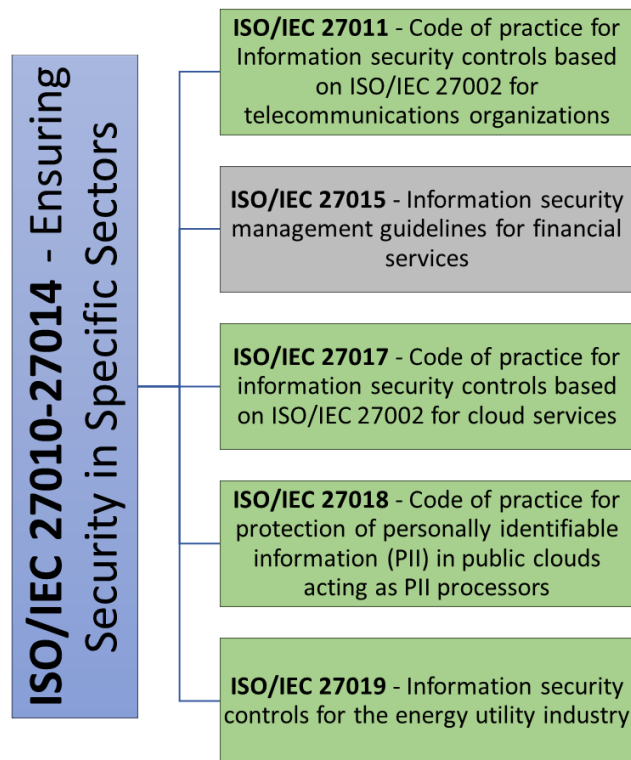


Figure 34 - ISO 27000 family - Security in Specific Sectors

After that there are specific guidelines for control activities, which can be divided into those dedicated to business continuity and supply chain security, and those dedicated to the forensic investigation phase following an incident.

Business continuity is another aspect often associated with information security. In general terms, it can be defined as the ability of an organisation to maintain or resume normal operations following a disruption. Although the focus is mainly on business, there is a close relationship with security measures, especially those related to disaster recovery procedures. While the latter focus solely on the IT infrastructure, business continuity covers the entire organisation and its processes. In short, the aim is to achieve the best business resilience, which must be an important part of risk management decisions. ISO 22301 deals with business continuity, but its rationale is deepened by ISO 27031 with regard to the responsiveness of the organisation's ICT systems. This guideline can be said to help protect availability before the other characteristics of cybersecurity.

Continuing in this order, the next ISOs can be conceived in a progression from the outside to the inside of the organisation. The subject is still cybersecurity, but from a different point of view. The first, ISO 27032, introduces different areas of cyber security such as network security, internet security and critical infrastructure cyber security. For each of these, the basics are provided and the interdependencies between the areas are outlined. The approach is general and introductory, as the intention is simply to provide the basic security tools that different actors in cyberspace should adopt. The creation of a common toolkit is a useful starting point for fostering cooperation on security issues and promoting the pursuit of a secure cyberspace. The next point of view concerns one of the areas just mentioned, that of network security. ISO 27033 is divided into several parts and tries to cover the different aspects of ICT network security from a technical point of view.

It is one of the most important guidelines for the design of a secure network, guiding

security architects in the management of the main risk scenarios. ISO 27039 integrates these more general aspects of network security by supporting the implementation of an IDPS (Intrusion Detection and Prevention System). From the global perspective, we then move to the inside of the organisation. The final point of view is that of the applications, whose security must follow very precise design principles, both in terms of in-house development and software purchased from third parties. ISO 27033 is dedicated to this and provides assistance in the implementation of security controls in the application development cycle (we speak of application security controls), from their introduction to their withdrawal, with particular attention to their maintenance.

Related to this, ISO 27036 covers, in a broader sense, all the relationships an organisation may have with its suppliers, not limited to software. It covers all dependencies with suppliers and identifies the appropriate requirements to be implemented for both parties. Much of the implementation guidance is dedicated to cloud service providers.

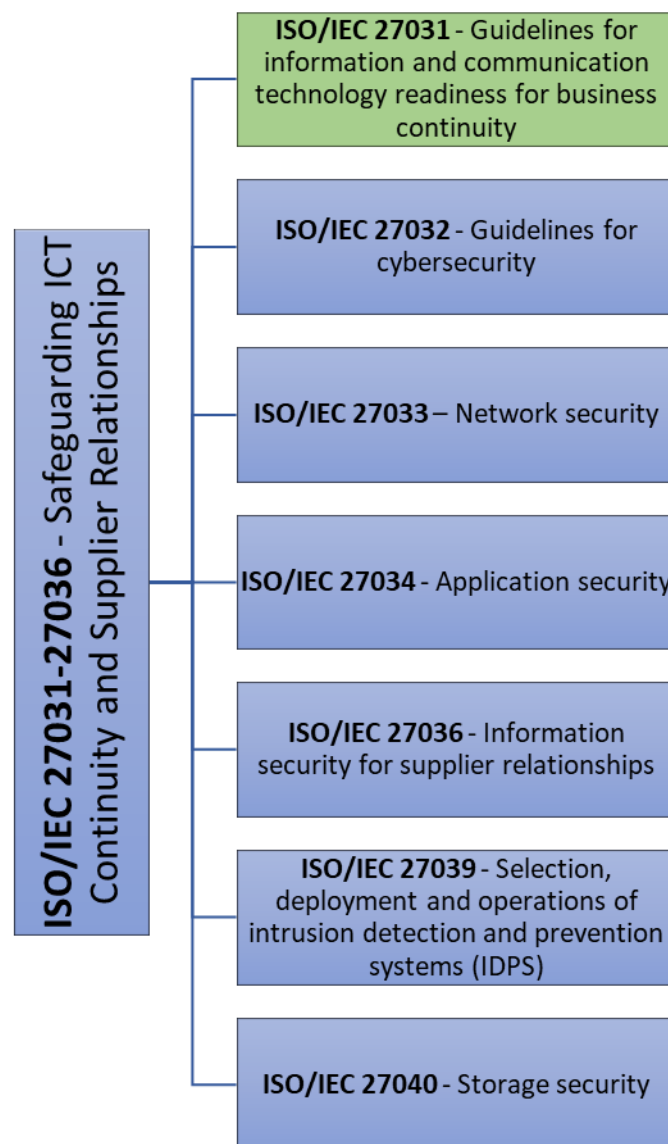


Figure 35 - ISO 27000 family - Safeguarding ICT Continuity and Supplier Relationships

Coming to the last block of ISOs in this review, we introduce the topic of digital evidence,

which is the result of decades of practices and procedures belonging to the different branches of digital forensics. To the extent that its studies have consolidated over time, it is possible to recall the definition that emerged from the famous Utica workshop, which represented the turning point for the consolidation of the discipline<sup>751</sup>.

Digital forensics is "the use of scientifically derived and proven methods for preserving, collecting, validating, identifying, analysing, interpreting, documenting, and presenting digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events that have been determined to be criminal, or helping to anticipate unauthorized actions that have been determined to be disruptive to planned operations"<sup>752</sup>. If the goal is to preserve the legal value of evidence, a high degree of proceduralization is necessary. Initially, digital forensic procedures were inspired by those that already existed for the physical analysis of the crime scene, of which digital evidence is now an important part<sup>753</sup>. This branch has gradually become independent, consolidating its own recognised practices<sup>754</sup>. To support the work of security analysts, this guide proposes a set of best practices and procedures. These steps are part of the overall incident management process, of which they are the final stage.

Following a schematisation suggested by a recent literature review, it is possible to place these ISOs within the process they help to define<sup>755</sup>. For this purpose, a distinction must be

---

<sup>751</sup> Taking Mark Pollitt's work as a starting point, it is possible to date digital forensics studies in different historical phases.

The prehistory, before 1985, was characterised by the reluctance of states to approach this new branch of investigation. Such activities were carried out by groups of volunteers. Moreover, at that time, computers were still a phenomenon limited to the industrial world and to a small circle of people. It was not until the first IBM PC was launched in the early 1980s that they became widely available. In the so-called infancy of digital forensics, police forces around the world were trying to organise themselves to prevent future developments. The decade from 1995 to 2005 was marked by significant technological development, brought about by the spread of modern communication networks and the Internet. This led to the first child pornography scandals. Since then, digital forensics has been recognised and regulated worldwide. One example is the Budapest Convention drawn up by the Council of Europe in 2001. For the full chapter see Mark Pollitt, 'A History of Digital Forensics', in *Advances in Digital Forensics VI*, ed. Kam-Pui Chow and Sujeet Sheno, IFIP Advances in Information and Communication Technology (Berlin, Heidelberg: Springer, 2010), 3–15, [https://doi.org/10.1007/978-3-642-15506-2\\_1](https://doi.org/10.1007/978-3-642-15506-2_1).

<sup>752</sup> 'A Road Map for Digital Forensic Research' (Utica, New York: Digital Forensic Research Workshop, 7 August 2001), 16, [https://dfrws.org/wp-content/uploads/2019/06/2001\\_USA\\_a\\_road\\_map\\_for\\_digital\\_forensic\\_research.pdf](https://dfrws.org/wp-content/uploads/2019/06/2001_USA_a_road_map_for_digital_forensic_research.pdf).

<sup>753</sup> Brian D. Carrier and E. Spafford, 'Getting Physical with the Digital Investigation Process', *International Journal of Digital Evidence* 2, no. 2 (2003): 5–12.

<sup>754</sup> Several practices emerged from the scientific literature more than a decade ago. See Siti Rahayu Selamat, Y. Robiah, and Shahrin Sahib, 'Mapping Process of Digital Forensic Investigation Framework' 8 (1 January 2008). Selamat, Siti Rahayu, Y. Robiah and Shahrin Sahib. Mapping Process of Digital Forensic Investigation Framework" 8 (1 January 2008). More recently, the OSCAR methodology, derived from the acronym of its phases, deserves mention: Obtain Information, Strategise, Collect Evidence, Analyse, Report. For a more detailed analysis of each step, see European Union Agency For Network And Information Security, 'Forensic Analysis Network Incident Response Toolset, Document for Students', December 2016, 6, [https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material/documents/2016-resources/exe2\\_forensic\\_analysis\\_ii-toolset](https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material/documents/2016-resources/exe2_forensic_analysis_ii-toolset); Sherri Davidoff and Jonathan Ham, *Network Forensics: Tracking Hackers through Cyberspace* (Upper Saddle River, NJ: Prentice Hall, 2012), 17–22.

<sup>755</sup> For a more complete review see Fran Casino et al., 'Research Trends, Challenges, and Emerging Topics of Digital Forensics: A Review of Reviews' (arXiv, 10 January 2022), 16–23, <https://doi.org/10.48550/arXiv.2108.04634>.



made between high-level guidelines, process guidelines and specific guidelines. The former are mainly concerned with providing definitions and an overview of the entire process. For example, a complete scan of the steps from the planning phase to the closure phase can be found in the first part of ISO 27035. Figure 36 depicts all phases of the incident management cycle.

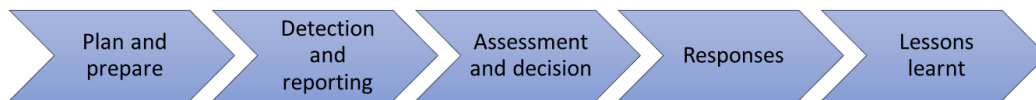


Figure 36 - ISO27035 - Incident Management Cycle

In short, the planning and preparation phase implies the existence of policies and a detailed incident response plan involving the appropriate people in the organisation and support mechanisms. Consequently, the follow-up phase implies the implementation of the planned control mechanisms, which usually consist of network and endpoint activity monitoring and logging systems. Armed with this knowledge, the responsible personnel can follow the procedures established after a security event has been classified as an incident. This mainly involves gathering additional information to rule out a false positive and collecting all activities that have taken place. If the incident is confirmed, response activities are initiated, and appropriate resources are assigned. These must ensure that all digital evidence is preserved, and that the existence of the incident is communicated to the authorities or other organisations. Once the incident is resolved, the opportunity must be taken to review the information management system and security controls.

Still at a high level, the same process is also detailed by ISO 27043, which distinguishes four classes of processes: Readiness, Initialisation, Acquisition, Investigation. The various phases shown in the diagram are subdivided into these classes and enriched at the level of principles.

The remaining guidelines increase the level of concreteness. As expected, some of them take a holistic view of the process. For example, ISO 27041 helps to identify the best investigation methods to meet the organisation's needs. For this reason, its guidance relates to the whole information process. However, ISO 27050 on electronic discovery requires a separate discussion. Since the digital information production process<sup>756</sup> may have quite different purposes, not necessarily related to the process of handling a security incident. Abstractly, an incident could correspond to the commission of a crime, so evidence of the crime should be identified, preserved, collected, and ultimately presented to the judicial authority. However, the reason for production could be for other reasons, such as a simple request from a third party who is entitled to it.

The latest ISOs all refer to a specific step in the incident management process. Related to the e-discovery process just mentioned, ISO 27037 looks at digital evidence management procedures, addressing a variety of devices. Next, ISO 27038 covers aspects of information redaction, i.e. the removal of personal data that is not necessary for the investigation.

---

<sup>756</sup> The process is divided into several stages: 1) identification; 2) preservation; 3) collection; 4) processing; 5) review; 6) production. The first step is to identify the information needed, based on its purpose. The information then needs to be protected from change and collected. Before production, the information may need to be processed to meet any imposed criteria. Any changes made must be tracked and compliance verified. The final step is to send the information to the requester.

Finally, ISO 27042 is fundamental to the interpretation of evidence, providing common elements for evaluation. It not only provides templates for carrying out this analysis, but also helps in writing the final report.

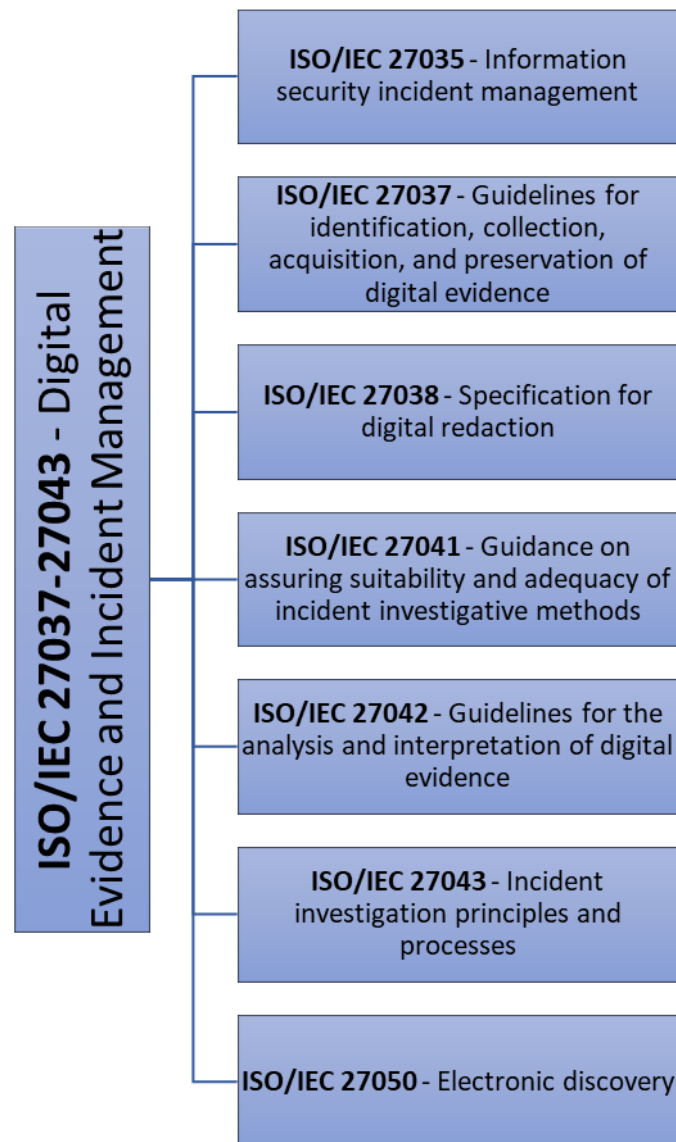


Figure 37 - ISO 27000 family - Digital Evidence and Incident Management

#### I.4 The NIST cybersecurity framework

Having devoted much space to introducing concepts and technical production at the international level, it is now possible to move on to the national level. However, the discussion of the National Cyber Security Framework requires some further preamble. Its highly technical nature requires an understanding of the functioning of the National Cybersecurity Framework, elaborated by CINI in collaboration with La Sapienza University of Rome, given the precise references introduced by the Italian legislator. It is therefore essential to refer to the cybersecurity framework developed by the American NIST, of which the Italian framework is a direct descendant and shares the same operating logic.

Founded in 1901 as part of the US Department of Commerce, the National Institute of Standards and Technology is one of the most important agencies for promoting innovation

and measuring physical and material phenomena<sup>757</sup>. With the proliferation of network technologies and the escalation of security issues, NIST's work also focused on cybersecurity. The starting point was Executive Order 13636, signed by then President Obama on 12 February 2013. Its Section 1 is an emblematic snapshot of the situation on the other side of the Atlantic at the time. "Repeated cyber intrusions into critical infrastructure demonstrate the need for enhanced cybersecurity. The cyber threat to critical infrastructure continues to grow and is one of the most serious national security challenges we face. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats"<sup>758</sup>.

Not unlike the more recent interventions that characterise European Union policy, the United States had long before the Old Continent recognised the need to take action to protect its critical infrastructure. On the one hand, the emphasis was on increasing the exchange of information on security incidents to improve its defences based on shared knowledge. On the other hand, there was a need for a technical reference tool to support cyber risk management.

As a result, the Director of NIST was tasked with developing methodologies and procedures to align business objectives and technology approaches to mitigate risk. The principles at the heart of this are the same as those that characterise the current standard, namely flexibility, repeatability, and better value for money. The result is a neutral framework that can adapt to any technology, while measuring performance in implementation. After an open review period that started on 1 July 2013, the first version was released to the public on 12 February 2014. Over time, several areas for improvement have been identified as technology advances. Consider, for example, the revolution brought about by the emergence of the Internet of Things (IoT), or the need to balance security measures with privacy<sup>759</sup>.

Incidentally, it was another piece of legislation that revived NIST's work. The so-called Cybersecurity Enhancement Act had authorised NIST to increase cooperation with the private sector in developing and updating the Cybersecurity Framework<sup>760</sup>. At the same time, it expanded its mandate to include the creation of checklists to assist federal agencies in the proper implementation of various technologies<sup>761</sup>.

---

<sup>757</sup> See 'National Institute of Standards and Technology', text, NIST, 20 November 2023, <https://www.nist.gov/>.

<sup>758</sup> 'Executive Order -- Improving Critical Infrastructure Cybersecurity', 12 February 2013, 1, <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

<sup>759</sup> For other insights sought over time, see 'Introduction to the Framework Roadmap', NIST, 13 April 2018, <https://www.nist.gov/cyberframework/online-learning/introduction-framework-roadmap>.

<sup>760</sup> Other areas of interest, such as digital identity, should also not be overlooked. NIST has published Special Publication (SP) 800-63-3 in three parts, to which a fourth, currently in draft form, will soon be added. See Paul Grassi, Michael Garcia, and James Fenton, 'Digital Identity Guidelines' (National Institute of Standards and Technology, 2 March 2020), <https://doi.org/10.6028/NIST.SP.800-63-3>. For the regulatory scope, see 'Public Law 113 - 274 - Cybersecurity Enhancement Act of 2014', Pub. L. No. 274, 274 (2014), <https://www.govinfo.gov/app/details/PLAW-113publ274>.

<sup>761</sup> The NIST Special Publication 800-70 had officially regulated the national checklist programme, explaining both the use of the checklists made available to technicians and the methodology for their development and submission to NIST for approval and subsequent dissemination. On the programme's official portal, it is possible to search and download checklists containing targeted security checks. See Stephen D Quinn et al., 'National Checklist Program for IT Products - Guidelines for Checklist Users and Developers' (Gaithersburg, MD: National Institute of Standards and Technology, February 2018), <https://doi.org/10.6028/NIST.SP.800-70r4>; 'NCP -

NIST's role as a key player in coordinating technical standardisation in the field of security has also been formally established in terms of international cooperation. These developments led to the release of a first update on 16 April 2018<sup>762</sup>.

A decade after version 1.0, version 2.0 has been released in February 2024.

Without claiming to be exhaustive, it is good to focus on its main components to understand the similarities of the national framework, and therefore the National Cybersecurity Perimeter. Although the objectives are similar in terms of the systems proposed by the ISO standards, there are some differences in terms of both terminology and methodology.

First, it should be noted that the subject of the ISO 27000 family is information security, while the American framework refers to the concept of cybersecurity. Despite the choice of language, the scope is roughly the same. The different use of terms changes where the focus is placed. While the definition of information security tends to emphasise the object to be protected, i.e. the information, talk of cybersecurity focuses on the process leading to its achievement, in all its phases<sup>763</sup>.

In terms of methodology, the NIST framework abstractly follows the stages of the Deming Cycle and provides a tool for describing an organisation's current cybersecurity posture. Although the tool was created to assist US critical infrastructure, it can be used by any type of organisation<sup>764</sup>.

The process focuses on identifying the current state, as this is the starting point for defining a state to be pursued. Implementation then becomes a journey broken down into a series of steps, each of which has its own priority according to the relationship between its effectiveness in preventing risk and its cost. As each reality has its own specificities in terms of risk management, the framework should not be seen as a "universal methodology". Rather, it should be seen as a versatile tool that can be adapted to different threats, vulnerabilities, and risk tolerance levels, depending on the context.

This initial complexity is compounded by the fact that there is no single way to use the framework. Not only can it be used by different organisations, but there are different ways of using it. Therefore, addressing the issue of compliance always requires appropriate contextualisation.

---

Information', accessed 26 November 2023, <https://ncp.nist.gov/general>.

<sup>762</sup> National Institute of Standards and Technology, 'Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1' (Gaithersburg, MD: National Institute of Standards and Technology, 16 April 2018), <https://doi.org/10.6028/NIST.CSWP.04162018>.

<sup>763</sup> Compare the two definitions from ISO 27000 and the NIST Framework respectively: information security as maintaining the confidentiality (3.10), integrity (3.36) and availability (3.7) of information; cybersecurity as the process of protecting information by preventing, detecting and responding to attacks.

<sup>764</sup> The following is the definition of critical infrastructure contained in the USA Patriot Act: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating effect on national security, national economic security, national public health or safety, or any combination of these matters". See 'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (Usa Patriot Act) Act of 2001', Pub. L. No. 107-56 (2001), 401, <https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf>. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56 (2001). [<https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf>](<https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf>). p. 401.

Nevertheless, it is possible to introduce the key components that provide a structured language for communicating cyber risk management issues.

The foundation of the entire framework is its core. At first glance, it may resemble a checklist of sorts, as it consists of a series of activities aimed at achieving specific cybersecurity outcomes. Despite the similarity, these are not mandatory actions to be taken. The list aims to provide as complete a picture as possible of the main possible cybersecurity actions. This will make them easier to identify and will also help to create a common language.

The Figure 38 illustrates the organisation of the High-Level Framework, showing the organisation of the actions. These are called sub-categories and are divided into categories, each of which is given a unique code to facilitate identification. As expected, each category in turn relates to a function, i.e. a high-level security objective to be pursued.

| Functions | Categories | Subcategories | Informative references |
|-----------|------------|---------------|------------------------|
| Govern    |            |               |                        |
| Identify  | ID.AM      | ID.AM-1       |                        |
|           |            | ID.AM-2       |                        |
|           | ID.BE      |               |                        |
| Protect   |            |               |                        |
| Detect    |            |               |                        |
| Respond   |            |               |                        |
| Recover   |            |               |                        |

Figure 38 - NIST 2.0 Cybersecurity Framework - Functions, Categories, Subcategories

The table can be said to be organised in an order from general to specific. On the left is the high-level function, while on the right is the specific action to be taken. These are not specified in detail but are accompanied by a series of informative references consisting of a series of directives or regulations. The overview is not exhaustive, but it helps to clarify the operational procedure.

Below is an example taken from the Identify function, which was the first function before the change made in version 2.0. The first category is dedicated to asset management, i.e. the identification of all the resources needed to pursue the business objectives. The first subcategory relates to the mapping of physical systems.

| Function      | Category                                                                                                                                                                                                                                                       | Subcategory                                                                   | Informative reference                                                                                                                                                                                                                                                                |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Identify (ID) | ID.AM: The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. | ID.AM-1: Physical devices and systems within the organization are inventoried | <ul style="list-style-type: none"> <li>• CIS CSC 1</li> <li>• COBIT 5</li> <li>• BAI09.01, BAI09.02</li> <li>• ISA 62443-2-1:2009 4.2.3.4</li> <li>• ISA 62443-3-3:2013 SR 7.8</li> <li>• ISO/IEC 27001:2013 A.8.1.1, A.8.1.2</li> <li>• NIST SP 800-53 Rev. 4 CM-8, PM-5</li> </ul> |

Figure 39 – NIST Cybersecurity Framework example

The aim of the identification function is to gain an understanding of how the organisation operates to properly assess cyber risk.

Like what has already been described for ISO 27001, it is necessary to analyse and understand the business context and the supporting resources, both technological and human. This knowledge then informs the development of the most appropriate governance, and the identification of security measures appropriate to the context.

This is mainly done through the second function, Protect, which covers the development and implementation of security measures to ensure the proper functioning of services. Each of its categories is specialised in covering one aspect of security, such as access management, both physical and digital, training or data security. As you can imagine, the range of activities is quite broad, in order to adapt to the security of each context. In order not to run the risk of trivialising aspects that require more careful consideration, I will simply refer you to the framework.

Once all the measures deemed most appropriate for a given context have been implemented, another need arises: to be able to detect any anomalies in good time. This is the purpose of the detect function, which aims to implement systems to identify any security events that may be relevant. All events must be properly logged to be analysed and classified as incidents. In general, there are three fundamental components to the correct performance of this function. First, roles and processes must be defined to ensure the ability to detect anomalies. This is followed by continuous monitoring, which must cover physical, personnel and digital activities, such as network operations or known asset vulnerabilities. As a result of this continuous logging, it is possible to timely classify a security event as an incident and then assess its impact on the organisation.

When faced with an incident that has been established through a variety of evidence, response procedures need to be activated. Accordingly, a response plan must be developed and maintained that defines the roles of the response team and the resources available to them. Escalation protocols must also be in place to be activated if the incident escalates to a higher level in the organisation. Another essential aspect is the communication of the incident to stakeholders or authorities. As analysed in chapter two, and as we will also see in the Italian National Cybersecurity Perimeter, this is a matter that is often regulated and indicated as a requirement by both European and national legislators. The basis of effective communication is a well-functioning internal response system and the ability to produce effective reports.

This follows the analysis of the accident, both in terms of its effects and its ultimate cause.

The ability to analyse the accident means identifying its indicators and gathering evidence to reconstruct and prove what happened.

However, the main consequence of effective analysis is mitigation, i.e. the prevention of further spread of the incident and the elimination of its root cause. The results of both analysis and mitigation are critical in a continuous improvement perspective, which is ideally the final step in completing proper mitigation. Response plans need to be properly updated so that the same situation does not happen again but can be prevented.

It should be emphasised that mitigation does not imply a return to normal functioning of the affected systems. For example, in the case of a ransomware attack, mitigation would result in containment of the attack, removal of the malware and recovery of data from a backup. However, this may not be sufficient to resume normal operations, which may require additional steps, such as restoring normal network connectivity that was interrupted during the attack to prevent its spread. This is the subject of the final function, known as recovery, which involves its own separate planning, complete with mechanisms for communicating the incident to the outside world and systems for improving procedures.

Although the recover function completes the cycle of responding to an incident, version 2.0 of the framework introduced the govern function, which is transverse to the others. Its purpose is to support the ongoing effort to integrate cybersecurity into business practices, that is, into strategies and policies. This is reminiscent of the logic of ISO 27000, which from the outset has devoted space to the issue of understanding the organisation's objectives, which must be pursued consistently with security. In other words, the government function leads to the prioritisation of the categories and subcategories of the other functions based on the best balance with respect to the mission to be pursued.

Now that the basics of the framework have been introduced, the other concepts that build on it can be introduced.

The first is the profile framework, which represents a selection of functions, categories and subcategories that are consistent with the organisation's requirements, risk tolerance and resources. As noted above, the framework is not a checklist to be applied mechanically, but needs to be contextualised for each user. Consequently, not all subcategories need to be selected, but only the most appropriate ones. This is useful not only to reflect the current state of the security posture, but also to prepare for the desired state. This usually corresponds to the adoption of more subcategories of the protection function, i.e. more security controls.

The second concept is tier, which can be defined as a way of describing how an organisation approaches its cybersecurity risk. In this respect, tier is a way to better define the context of the profiles. However, it should be made clear that it is not an assessment of the level of maturity achieved, but rather the integration of cybersecurity into the business in a way that is consistent with the business and resources. Depending on the level of sophistication and consistency of its cybersecurity practices, an organisation can place itself in four different tiers. These are numbered from 1 to 4 and correspond to an increasing level of integration, which is assessed from three different perspectives.

The first is the risk management process, which aims to describe the level of formalisation of risk management procedures in general, without reference to cyber risk, in particular. The next step is to describe the level of integration of cyber risk into the broader risk management process. The aim is to examine whether cyber risk is addressed through formalised processes and what information is considered to support this. This is referred to as an integrated risk

management programme. Although the two perspectives may seem similar, they can be thought of as moving from the general to the specific. The former considers the entire risk management process without distinguishing between types of risk. The only reference to cybersecurity is in the assessment of how risk information can affect cyber measures. In technical terms, this means assessing whether cyber measures are informed or not. The second perspective, on the other hand, looks holistically at the integration of cyber risk in the organisation. This includes, for example, assessing the overall level of awareness and coverage of internal information sharing. Specifically, it examines the relationship between awareness and the processes used to assess the security posture of its own assets. The higher the level, the closer the integration between the two aspects, which are formalised in specific policies.

Finally, the organisation's external participation in the ecosystem in which it operates is considered. At the lowest levels, the organisation has little awareness of its own placement, which increases as its contribution to the outside world increases. This brings to the fore the issue of the supply chain, which not only needs to be understood, but above all needs to be harnessed to act appropriately in providing security for the organisation and its suppliers.

Figure 40 summarises the difference between these perspectives, broken down into their constituent elements.



|                                    |                                                                  | Tier 1: Partial | Tier 2: Risk Informed                               | Tier 3: Repeatable                                    | Tier 4: Adaptive                                                      |
|------------------------------------|------------------------------------------------------------------|-----------------|-----------------------------------------------------|-------------------------------------------------------|-----------------------------------------------------------------------|
| Risk Management process            | Risk management practices                                        | Not formalised  | Approved but not as a organisational-wide policy    | Formal policy                                         | Formal policy                                                         |
|                                    | Cybersecurity activities                                         | Not informed    | Informed by business risk objectives                | Updated through the risk management process           | Updated through a process of continuous improvement                   |
| Integrated Risk Management Program | Awareness of cybersecurity risk                                  | Limited         | Yes, but not through a organisational-wide approach | Formal policy                                         | Risk-informed policy                                                  |
|                                    | Internal Cybersecurity information                               | No              | Yes, but only on informal basis                     | Yes, on regular basis and throughout the organisation | Yes, on regular basis and throughout the organisation                 |
|                                    | Cyber risk assessment                                            | No              | Yes, but typically not repeatable                   | Yes, it occurs consistently                           | Yes, as an inherent part of the organisational culture                |
| External Participation             | Understanding of the organisational role in the larger ecosystem | No              | Only of its own dependencies or dependents          | Yes                                                   | Yes, and contribute to the community's broader understanding of risks |
|                                    | External collaboration                                           | No              | Yes, but information are not shared externally      | Yes                                                   | Yes                                                                   |
|                                    | Supply chain risks                                               | Not understood  | Understood, but not exploited consistently          | Understood and usually exploited                      | Understood and exploited through external mechanism                   |

Figure 40 – NIST Cybersecurity Framework - Tiers

As announced at the outset, the Framework has been revised and replaced by its version 2.0, which was published in February 2024. Although this examinations simply aims to share the logic behind the NIST framework, the main changes between the old and the new version must be briefly presented. Although only a few years old, NIST has grasped the profound social and technological changes we are facing and has tried to provide appropriate responses to keep the framework relevant.

Undoubtedly, the most important change has been the adaptation of the scope, which is reflected in the title of the document. Although the Framework had started as a tool to support critical infrastructure, it had become more widely used, not only nationally, but especially internationally. This widespread use had soon led to the Framework being considered as a recognised standard, despite its narrower scope. Hence the name changes

from 'Framework for Improving Critical Infrastructure Cybersecurity' to 'Cybersecurity Framework', in order to shift the focus to any type of organisation.

At the same time, the entire structure of the document underwent a major restructuring of the references to consider all the other standards that have been developed in the meantime on related topics<sup>765</sup>. The new role of the tool is reinforced by improved implementation support, with examples for each subcategory and guidance on how to create customised profiles for the organisation.

No less important is the updating of functions, categories, and sub-categories to take account of new security requirements. It is clear that there is an attempt to take a holistic approach to cybersecurity, which must be embedded in the organisation in the pursuit of its objectives and in its relationships with its stakeholders. This has already been considered above with reference to the new Government function and the new 'Improve' category under the Identify function. All of this points to a more pronounced focus on security as a holistic endeavour to be integrated under different profiles, such as supply chain and privacy<sup>766</sup>.

### I.5 A Brief History of the Italian National Cybersecurity Framework

The global significance of the NIST Cybersecurity Framework has triggered a series of similar developments in many countries, including Italy. Through a joint working group led by the Research Centre of Cyber Intelligence and Information Security at the University of Rome La Sapienza and the Cybersecurity National Lab (CINI) and composed of both public and private entities<sup>767</sup>.

Finally, we should not forget the support provided by the Department of Information for Security of the Presidency of the Council of Ministers, where the first Italian cybersecurity framework was born<sup>768</sup>.

Although the basic concepts were no different from those of the NIST framework, the result had the added value of being from the outset a comprehensive tool for application by organisations of different sectors and sizes. The basics are expanded and accompanied by further clarifications useful for use. For example, special attention is paid to profiles. Progressive implementation towards the desired profile is guided through the identification of priority levels (LOW, MEDIUM and HIGH) into which the different subcategories are placed. A measure is urgent when its ability to reduce the impact of a risk is high for the same implementation cost. Consequently, the ease of implementation is also considered when calculating priority. The most urgent actions are always those with the highest benefit and lowest implementation cost, considering the technical maturity of the organisation. Priority

---

<sup>765</sup> For example, the development of a framework dedicated to the risk management of artificial intelligence can be recalled. See Elham Tabassi, 'Artificial Intelligence Risk Management Framework (AI RMF 1.0)', *NIST*, 26 January 2023, <https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-ai-rmf-10>.

<sup>766</sup> The privacy theme will be strengthened in particular through better coordination with the National Institute of Standards and Technology, 'Nist Privacy Framework:: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0' (Gaithersburg, MD: National Institute of Standards and Technology, 16 January 2020), <https://doi.org/10.6028/NIST.CSWP.01162020>.

<sup>767</sup> On the public side, it is worth mentioning the participation of all public agencies involved in the country's digitisation aspects. These include AgID, the Data Protection Agency, the Ministry of Economic Development and CERT-PA.

<sup>768</sup> Research Center of Cyber Intelligence and Information Security and CINI Cybersecurity National Lab Consorzio Interuniversitario Nazionale per l'Informatica, '2015 Italian Cyber Security Report', February 2016, [https://www.cybersecurityframework.it/sites/default/files/CSR2015\\_ENG.pdf](https://www.cybersecurityframework.it/sites/default/files/CSR2015_ENG.pdf).

is not an absolute value, but relative to a given organisational reality.

Complexity within the organisation is also represented by the concept of maturity. The implementation of a subcategory does not always correspond to a Boolean value but can consist of a wider range of situations. In other words, it is not only significant whether a subcategory has been implemented or not, but how it has been implemented<sup>769</sup>.

The addition of these concepts results in the following framework table. The absence of the government function is due to the fact that the Italian framework has not yet been updated. At the same time, it should be noted that the choice of four levels of sophistication does not mean that each subcategory must necessarily reach this level of detail. As mentioned above, some subcategories may not be divided into levels, or may even be divided into only two maturity levels.

| Functions | Categories | Subcategories | Priority Levels | Maturity Levels |    |    |    | Informative references | Guidelines |
|-----------|------------|---------------|-----------------|-----------------|----|----|----|------------------------|------------|
|           |            |               |                 | M1              | M2 | M3 | M4 |                        |            |
| Identify  | ID.AM      | ID.AM-1       |                 |                 |    |    |    |                        |            |
|           |            | ID.AM-2       |                 |                 |    |    |    |                        |            |
|           | ID.BE      |               |                 |                 |    |    |    |                        |            |
| Protect   |            |               |                 |                 |    |    |    |                        |            |
| Detect    |            |               |                 |                 |    |    |    |                        |            |
| Respond   |            |               |                 |                 |    |    |    |                        |            |
| Recover   |            |               |                 |                 |    |    |    |                        |            |

Figure 41 - Italian Cybersecurity Framework - Components

To summarise briefly, any organisation can use the table by following a series of steps. The first is to identify the relevant functions, categories and sub-categories based on the context of the production sector, activity, and geographical location. For each of the identified sub-categories, priority levels need to be established, considering the benefits and costs of implementation. At least for the high priority subcategories, guidelines should also be established to support proper implementation. This is an additional support, shown in the last column on the right, missing in the NIST framework and added by the Italian framework, which pays more attention to user-friendliness. A high priority should also correspond to a higher level of detail in terms of identifying maturity levels. These should be identified at least for the high priority subcategories to be aware of both the current level of implementation and the target to be achieved. Once the gap between the two has been defined, steps to close it can be planned.

In addition to the extension of the basic concepts, the Italian framework is already accompanied by a working guide addressed to the most representative categories of the Italian landscape. The second part of the guide not only presents the core framework, but also contextualises it so that it can be applied by small and medium-sized enterprises, which are the most representative actors on the Italian scene. In this way, they are confronted with simplified steps. For example, subcategories that are not appropriate for an SME have been removed, and all those identified as high priority are already accompanied by implementation guidelines and a description of maturity levels. Of course, each organisation will have to

<sup>769</sup> Please refer to the Framework for an in-depth explanation. See Research Center of Cyber Intelligence and Information Security and CINI Cybersecurity National Lab Consorzio Interuniversitario Nazionale per l'Informatica, '2015 Italian Cyber Security Report - Un Framework Nazionale per la Cyber Security', February 2016, 15–18, [https://www.cybersecurityframework.it/sites/default/files/CSR2015\\_web.pdf](https://www.cybersecurityframework.it/sites/default/files/CSR2015_web.pdf).

consider its own context and make some adjustments, as it cannot fit perfectly into the proposed profile, which is still the result of an average.

The great comprehensiveness of the Italian framework is also due to its ability to cover regulatory aspects. The third part deals with specific aspects related to sectoral contexts of application. While the first concerns the proper conduct of cyber risk analysis, which is accompanied by the question of the correct insurance tools, a great deal of space is devoted to the issues of privacy and the management of classified information. Each need implied by the regulations identified is broken down and assigned to the most appropriate subcategories. Other relevant sectors are banking and public administration. In particular, the first framework correctly identified the role of the Agenzia per l'Italia Digitale (AgID) in the elaboration of guidelines for public administration<sup>770</sup>.

For this reason, the framework does not include a profile for the public administration. Following the Prime Minister's directive of 1 August 2015 requiring the public administration to adopt minimum security standards, AgID had issued its own circular containing a minimum profile based on the National Cybersecurity Framework<sup>771</sup>.

Despite these marginal developments promoted by the legislator, the framework has struggled to take root in the Italian economic fabric, "which is, for the most part, made up of a galaxy of medium, small and very small companies, in which these specific personnel are not present due to structural and turnover problems". [...]. This galaxy of companies is the backbone of our economy and the foundation of Italian production chains, the architects of our national prosperity"<sup>772</sup>. Their inherent insecurity risks becoming a systemic vulnerability for the country, so the same working group behind the Framework had come up with an alternative way to support the security of the smaller realities. Take the example of the so-called Cyber Essentials<sup>773</sup>, developed and regularly updated by the UK National Cyber Security Centre, essential cybersecurity controls have been identified<sup>774</sup>.

These represent cybersecurity practices that, if ignored or improperly implemented, would lead to a significant increase in cyber risk. The aim is therefore to ensure that they can be easily implemented, even by people without specific cybersecurity knowledge. There are fifteen controls in total, which are mapped to the Framework's subcategories.

The last update of the Framework dates back to 2019, when was published the 2.0

---

<sup>770</sup> See Article 14-bis of Legislative Decree No. 82 of 7 March 2005, better known as the Digital Administration Code (CAD), which lists the functions of the Agency. These include the adoption of rules, standards and technical guidelines and the verification of their compliance through supervisory powers.

<sup>771</sup> For the full text of the circular, later published in the Official Gazette, see Agenzia per l'Italia digitale, 'CIRCOLARE 18 Aprile 2017, n. 2/2017 - Sostituzione Della Circolare n. 1/2017 Del 17 Marzo 2017, Recante: «Misure Minime Di Sicurezza ICT per Le Pubbliche Amministrazioni. (Direttiva Del Presidente Del Consiglio Dei Ministri 1° Agosto 2015)»', 18 April 2017, <https://www.gazzettaufficiale.it/eli/id/2017/05/05/17A03060/sg>.

<sup>772</sup> My translation from Research Center of Cyber Intelligence and Information Security and CINI Cybersecurity National Lab Consorzio Interuniversitario Nazionale per l'Informatica, '2016 Italian Cybersecurity Report - Controlli Essenziali di Cybersecurity', March 2017, 3, <https://www.cybersecurityframework.it/sites/default/files/csr2016web.pdf>.

<sup>773</sup> National Cyber Security Centre, 'Cyber Essentials: Requirements for IT Infrastructure v3.1', April 2023, <https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf>.

<sup>774</sup> Research Center of Cyber Intelligence and Information Security and CINI Cybersecurity National Lab Consorzio Interuniversitario Nazionale per l'Informatica, '2016 Italian Cybersecurity Report - Controlli Essenziali di Cybersecurity'.

version<sup>775</sup>, which had become necessary to maintain the coordination of the instrument with respect to the entry into force of the GDPR in 2018. The new version highlights the differences with the previous version and proposes controls, inspired by the new regulation, to ensure full compliance after implementation. It also provides a profile for all organisations that fall within the scope of the GDPR. This indicates the most appropriate sub-categories, prioritising them and making them mandatory.

This is where the work of the research team from the University of Genoa in the ERACLITO project comes in. The contribution of mapping compliance obligations stemming from the Perimeter Regulation can complement the National Cybersecurity Framework or other international standards.

---

<sup>775</sup> Research Center of Cyber Intelligence and Information Security and CINI Cybersecurity National Lab Consorzio Interuniversitario Nazionale per l'Informatica, 'Framework Nazionale per La Cybersecurity e La Data Protection', February 2019, [https://www.cybersecurityframework.it/sites/default/files/framework2/Framework\\_nazionale\\_cybersecurity\\_data\\_protection.pdf](https://www.cybersecurityframework.it/sites/default/files/framework2/Framework_nazionale_cybersecurity_data_protection.pdf).

I.6 Compliance requirements from the Italian Cybersecurity Perimeter

| Original italian denomination                                                 | English translation                                                            | Acronym used in the text |
|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------|--------------------------|
| Agenzia per la Cybersicurezza Nazionale                                       | National Cyber Security Agency                                                 | ACN                      |
| Autorità NIS competenti di settore                                            | NIS Sectorial Competent Authorities                                            |                          |
| Centrali di Committenza                                                       | Central purchasing bodies                                                      |                          |
| Centri di Valutazione del Ministero dell'interno e del Ministero della difesa | Evaluation Centres of the Ministry of the Interior and the Ministry of Defence | CVs                      |
| Centro di Valutazione e di Certificazione Nazionale                           | National Evaluation and Certification Centre                                   | CVCN                     |
| Comitato Interministeriale per la Cybersicurezza                              | Interministerial Committee for Cybersecurity                                   | CIC                      |
| Comitato Interministeriale per la Sicurezza della Repubblica                  | Interministerial Committee for the Security of the Republic                    |                          |
| Comitato tecnico di raccordo                                                  | Technical Liaison Committee                                                    |                          |
| Commissione di accreditamento                                                 | Accreditation Commission                                                       |                          |
| Dipartimento delle informazioni per la sicurezza                              | Department of Security Information                                             | DIS                      |
| Fornitori di Servizi Digitali                                                 | Digital Service Provides                                                       | DSP                      |
| Forze di polizia                                                              | Law enforcement                                                                |                          |
| Laboratorio Accreditato di Prova                                              | Accredited Test Laboratory                                                     | LAP                      |
| N.A.                                                                          | Computer Security Information Response Team                                    | CSIRT                    |
| Operatori di Servizi Essenziali                                               | Operator of Essential Services                                                 | OES                      |

|                                                                                                                                              |                                                                                                                                      |  |
|----------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|--|
| Organi Costituzionali                                                                                                                        | Constitutional bodies                                                                                                                |  |
| Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione                                          | The body of the Ministry of the Interior for the security and regularity of telecommunication services                               |  |
| Presidente del Consiglio dei Ministri                                                                                                        | President of the Council of the Ministers                                                                                            |  |
| Strutture specializzate in tema di protezione di reti e sistemi delle amministrazioni da cui dipendono le Forze di polizia e le Forze armate | Specialised structures for the protection of networks and systems of the administrations on which the police and armed forces depend |  |

Table 1 - Functional requirements for the Perimeter subjects

| Source of law                                        | Subject to the requirement |           | Requirement                                                                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Recipient of information                  | Controls                                                                                                                                                                                                                                  |
|------------------------------------------------------|----------------------------|-----------|--------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| D.P.C.M. 30 July 2020, n. 131, art. 2                | Constitutional bodies      |           | Joining the security perimeter                                                                   | Constitutional Bodies, if they wish to adopt security measures similar to those provided for the Perimeter Subjects, may enter into special agreements with the President of the Council of Ministers for this purpose.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | President of the Council of the Ministers | 1. A Constitutional body wants to adopt security measures similar to those provided for the Perimeter subjects<br>2. A secret agreement with the President of the Council of the Ministers is stipulated                                  |
| D.P.C.M. 30 July 2020, n. 131, art. 3,4 c. 1 let. a) | Identified administrations | sectorial | Identification of essential functions and services                                               | The identified administrations, each in its own area of competence, shall identify essential functions and services that depend on networks, information systems or computer services, the disruption or impairment of which could be detrimental to national security. The services may be directly relevant or may be performed or provided by supervised entities or operators, including private ones.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | President of the Council of the Ministers | 1. Essential ICT-dependent functions and services are identified for each sector                                                                                                                                                          |
| D.P.C.M. 30 July 2020, n. 131, art. 3,4 c. 1 let. b) | Identified administrations | sectorial | Assessing the impact of an incident on the essential function or service                         | The sectorial administrations must assess the impact of an incident on the essential function or service. At this end, the sectorial administrations must consider:<br>1) the negative effects of the disconnection of the essential function or service. Several factors can be evaluated to assess them, like the territorial extent of the essential function or service, the number and type of users potentially affected, the guaranteed service levels, if any, the possible economic impact;<br>2) the negative effects of the impairment of the performance of the essential function or service. In this case, the consequences of the lack of availability, integrity or of the confidentiality of the data must be evaluated;<br>3) the possibility to mitigate the interruption or the impairment of the essential function or service. The availability of alternatives and the time required to restore the service are essential elements of the assessment. | President of the Council of the Ministers | 1. The negative effects of the disconnection of the essential function or service are assessed<br>2. The negative effects of the impairment of the essential function or service are assessed<br>3. Mitigation possibilities are assessed |
| D.P.C.M. 30 July 2020, n. 131, art. 3,4 c. 1 let. c) | Identified administrations | sectorial | Identification of essential functions and services with the greatest impact on national security | The sectorial administrations sort the essential functions and services according to the impact of their interruption or impairment. The possibility to mitigate the impact is considered.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | President of the Council of the Ministers | 1. Essential functions and services are sorted according to the impact of their interruption or impairment                                                                                                                                |
| D.P.C.M. 30 July 2020, n.                            | Identified                 | sectorial | Identification of entities                                                                       | The sectorial administrations follow the list of essential                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | President of the Council of               | 1. Entities which provide essential                                                                                                                                                                                                       |

|                                              |                                                                                         |                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                           |                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------|-----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 131, art. 3,4 c. 1 let. d)                   | administrations                                                                         | performing essential functions or services                                                                   | functions and services and identify the entities which provide each one of them.                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | the Ministers                             | functions and services are identified                                                                                                                                                                                                                                                                                                                                                                                      |
| D.P.C.M. 30 July 2020, n. 131, art. 3,5 c. 1 | Identified administrations                                                              | List of entities performing essential functions or services                                                  | The identified administrations prepare a list of entities to be included in the perimeter and transmit it to the CIC, within 30 days of the inclusion of each addressee in the list. The communication shall indicate the essential function or the essential service in relation to the performance of which the entity has been included in the list.                                                                                                                                                                                            | CIC                                       |                                                                                                                                                                                                                                                                                                                                                                                                                            |
| D.P.C.M. 30 July 2020, n. 131, art. 5 c. 2   | CIC                                                                                     | Proposal of the list of entities performing essential functions or services                                  | The CIC proposes to the President of the Council of the Ministers a list of entities performing essential functions or services to be adopted. When necessary, updates are proposed.<br>The text of the article must be read in the light of the amendments of the D.L. 81 of 2021. In particular, art. 4 c. 6 of the D.L. assigns all the functions of the CISR related to the National Cybersecurity Perimeter (Comitato Interministeriale per la Sicurezza della Repubblica) to the new CIC (Comitato Interministeriale per la Cybersicurezza). | President of the Council of the Ministers | 1. A list of entities performing essential functions or services is proposed to the President of the Council of the Ministers                                                                                                                                                                                                                                                                                              |
| D.P.C.M. 30 July 2020, n. 131, art. 5 c. 2   | President of the Council of the Ministers                                               | Adoption of the list of entities performing essential functions or services                                  | The President of the Council of the Ministers adopts the list of entities performing essential functions or services with D.P.C.M. This act is secret and not subject to publication.                                                                                                                                                                                                                                                                                                                                                              |                                           | 1. A list of entities performing essential functions or services is adopted by the President of the Council of the Ministers with D.P.C.M.                                                                                                                                                                                                                                                                                 |
| D.P.C.M. 30 July 2020, n. 131, art. 8        | ACN                                                                                     | Templates to describe the ICT components                                                                     | The ACN prepares the template to describe the ICT components.<br>The template also helps to identify the needed information which each perimeter entity have to notify to the ACN.                                                                                                                                                                                                                                                                                                                                                                 |                                           | 1. The template to describe the ICT components is prepared by the ACN                                                                                                                                                                                                                                                                                                                                                      |
| D.P.C.M. 30 July 2020, n. 131, art. 5 c. 3   | ACN                                                                                     | Notification of inclusion in the perimeter                                                                   | The ACN notifies those on the list of their inclusion in the perimeter within 30 days of their inclusion. The list of entities is also communicated to the body of the Ministry of the Interior for the security and regularity of telecommunication services.<br>The model to describe the ICT components is sent together with the notification.                                                                                                                                                                                                 | Perimeter entity                          | 1. The new perimeter entity is notified of its inclusion in the perimeter<br>2. The new perimeter entity receives the templates to carry out the description of its identified ICT assets<br>3. The competent identified administration is notified of the inclusion<br>4. The body of the Ministry of the Interior for the security and regularity of telecommunication services receives the up-to-date list of entities |
| D.P.C.M. 30 July 2020, n. 131, art. 6        | Inter-ministerial table for the implementation of the national cyber security perimeter | Establishment of the inter-ministerial table for the implementation of the national cyber security perimeter | The Inter-Ministerial Table for the Implementation of the National Cybersecurity Perimeter is established to support the Technical CISR. The Board is chaired by a Deputy Director General of the ACN and is composed of two representatives from each CIC administration, one representative from each of the two agencies and two representatives from the other Ministries concerned from time to time.                                                                                                                                         | Technical CISR                            | 1. The Inter-Ministerial Table for the Implementation of the National Cybersecurity Perimeter is established                                                                                                                                                                                                                                                                                                               |
| D.P.C.M. 30 July 2020, n. 131, art. 7        | Perimeter entities                                                                      | List of ICT assets                                                                                           | The entities included in the perimeter prepare and update, at least once a year, the list of ICT assets under their responsibility, indicating their networks, information systems and IT services. Upon receipt of the information of inclusion in the perimeter, the perimeter entity identifies the ICT assets required to perform the essential function or service. To this end, they consider both the impact of an incident on the ICT asset and the dependencies with ICT systems                                                          |                                           | 1. The perimeter entities carry out a risk assessment to assess the impact of an incident on the ICT assets they use to provide an essential function or service<br>2. According to the results of the risk assessment, the perimeter entities prepare the list of ICT assets under their                                                                                                                                  |



|                                                                                                                                   |                                                                                                        |                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                         |                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                   |                                                                                                        |                                                            | belonging to other entities. The impact must be assessed in terms of limiting operations or compromising the availability, integrity or confidentiality of data.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                         | responsibility                                                                                                                                                                                                                                                                                                                                                                           |
| D.P.C.M. 30 July 2020, n. 131, art. 9, c. 1                                                                                       | Perimeter entities                                                                                     | Communication of the list of ICT assets                    | Within six months of receiving notification of their inclusion in the list, perimeter entities transmit to ACN their lists of ICT assets. The communication is made through ACN's digital platform.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | ACN                     | 1. The perimeter entities upload the list of ICT assets to the ACN's platform, within six months of receiving notification of their inclusion in the list                                                                                                                                                                                                                                |
| D.P.C.M. 30 July 2020, n. 131, art. 9, c. 2,3                                                                                     | The body of the Ministry of the Interior for the security and regularity of telecommunication services | Access to the platform                                     | The body of the Ministry of the Interior for the security and regularity of telecommunication services accesses the lists via the digital platform and provides the lists for the Ministry on the same platform.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | ACN                     | 1. The body of the Ministry of the Interior of the Ministry of the Interior for the security and regularity of telecommunication services has the necessary authorization and credentials to access the lists via the digital platform<br>2. The body of the Ministry of the Interior provides the lists concerning the Ministry                                                         |
| D.P.C.M. 81 art. 3 cc. 1-4 and<br>D.L. 105 of 2019 art. 1 c. 3-bis (added by D.L. 115 of 2022, better known as decreto aiuti bis) | Perimeter entities                                                                                     | Mandatory notification of incidents                        | The perimeter entities notifies the incidents impacting ICT assets within the perimeter or information systems or IT services that share security functions, resources, computation or memory, or basic software (OS or virtualization) with ICT assets to the CSIRT at the ACN. Notification must be made within 6 hours (incidents in Table 1 of Annex A) or 1 hour (incidents in Table 2 of Annex A). Incidents impacting networks, information systems, and IT services owned by a perimeter entity but located outside the perimeter must also be notified. Notification must be made within 72 hours. Exceptions are incidents impacting networks, information systems, and IT services of the Ministry of the Defence. The provisions of D.P.C.M. 81 should be applied, insofar as they are compatible. | CSIRT                   | 1. High severity incidents impacting on ICT assets within the perimeter are notified within 1 hour<br>2. Other incidents impacting on ICT assets within the perimeter are notified within 6 hour<br>3. Incidents impacting on ICT assets outside the perimeter are notified within 72 hour<br>4. The appropriate taxonomy from the D.P.C.M. or from the ACN is used for the notification |
| D.L. 105 of 2019 Art. 1 c. 3-bis (added by D.L. 115 of 2022, better known as decreto aiuti bis)                                   | ACN (in the figure of the general manager)                                                             | Incident taxonomy                                          | The ACN prepares the taxonomy of reportable incidents regarding relevant non-perimeter networks, information systems, and IT services is prepared. The perimeter entities adopt the taxonomy and use it while notifying security incidents.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Perimeter entities      | 1. The taxonomy of reportable incidents regarding relevant non-perimeter networks, information systems, and IT services is prepared by the ACN                                                                                                                                                                                                                                           |
| D.P.C.M. 81 art. 3 c. 5                                                                                                           | Perimeter entities                                                                                     | Integration of mandatory notification of incidents         | The perimeter entities supplement the notification in a timely manner once additional elements become known.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | CSIRT                   | 1. Additional elements to support the notification of the incident are provided by the perimeter entity when discovered                                                                                                                                                                                                                                                                  |
| D.P.C.M. 81 art. 3 c. 7                                                                                                           | Perimeter entities                                                                                     | Integration of mandatory request notification of incidents | At the request of the CSIRT, the perimeter entities supplement the notification within 6 hours of the request, if the incident is not subject to the investigative secrecy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | CSIRT                   | 1. The incident is not subject to the investigative secrecy<br>2. The incident notification is supplemented by the perimeter entity at the request of the CSIRT within 6 hours of the request                                                                                                                                                                                            |
| D.P.C.M. 81 art. 3 c. 8                                                                                                           | Perimeter entities                                                                                     | Notification of the restoration of impacted ICT assets     | When impacted ICT assets are restored, the perimeter entities notifies it to the CSIRT at ACN, if the incident is not subject to the investigative secrecy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | CSIRT                   | 1. The incident is not subject to the investigative secrecy<br>2. The restoration of the impacted ICT assets is notified to the CSIRT by the perimeter entity                                                                                                                                                                                                                            |
| D.P.C.M. 81 art. 3 c. 8                                                                                                           | Perimeter entities                                                                                     | Notification of incident to staff                          | The perimeter entities notify the security incidents to                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Personnel for perimeter | 1. The personnel of the perimeter                                                                                                                                                                                                                                                                                                                                                        |

|                                                     |                    |                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                        |                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------|--------------------|---------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                     |                    | for perimeter implementation                                                                                  | their personnel appointed for the perimeter implementation (security measure ID.AM-6).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | implementation of the perimeter entity                                                                 | entity appointed to the perimeter implementation is notified about security incidents                                                                                                                                                                                                                             |
| D.P.C.M. 81 art. 5 c. 1 and D.L. 65 of 2018 art. 7. | ACN                | Forwarding of incident notifications                                                                          | The ACN forwards the incident notifications to the body of the Ministry of the Interior for the security and regularity of telecommunications services (Article 7-bis of Decree-Law No. 144 of July 27, 2005, converted, with amendments, by Law No. 155 of July 31, 2005).                                                                                                                                                                                                                                                                                                                                                                                                         | The body of the Ministry of the Interior for the security and regularity of telecommunication services | 1. Incidents notifications are forwarded by the ACN to the the body of the Ministry of the Interior for the security and regularity of telecommunications services                                                                                                                                                |
| D.P.C.M. 81 art. 8 c.1 let. a)                      | Perimeter entities | Implementation of security measures (Annex B, Appendix 2, Category A)                                         | The perimeter entities implements the urgent security measures (identified in Annex B, Appendix 2, Category A) within 6 months from the date of transmission of ICT asset list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                        | 1. Urgent security measures are implemented by perimeter entities within 6 months from the date of the transmission of ICT assets list                                                                                                                                                                            |
| D.P.C.M. 81 art. 8 c. 1 let. b)                     | Perimeter entities | Implementation of security measures (Annex B, Appendix 2, Category B)                                         | The perimeter entities implements the non-urgent security measures (identified in Annex B, Appendix 2, Category B) within 30 months from the date of transmission of ICT assets list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                        | 1. Non-urgent security measures are implemented by perimeter entities within 30 months from the date of the transmission of ICT assets list                                                                                                                                                                       |
| D.P.C.M. 81 art. 8 c. 2                             | Perimeter entities | Notification of successful implementation of security measures                                                | The perimeter entities notify the successful implementation of security measures to the ACN through its digital platform.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | ACN                                                                                                    | 1. The successful implementation of security measures is notified to the ACN via its digital platform                                                                                                                                                                                                             |
| D.P.C.M. 81 art. 8 c. 4                             | Perimeter entities | Assessment of the need for implementation of new security measures following the update of the ICT asset list | The perimeter entities assess their need to implement new security measures as a result of updating the list of ICT assets. If yes, they proceed to implement possible urgent and non-urgent security measures, according to the procedures of art. 8 c. 1.                                                                                                                                                                                                                                                                                                                                                                                                                         | ACN                                                                                                    | 1. After an update of their ICT assets the perimeter entities assess their need to implement new security measures<br>2. If the implementation is necessary, the perimeter entities implement the urgent and non-urgent security measures<br>3. The procedure in D.P.C.M. 81 art. 8 is observed                   |
| D.P.C.M. 81 art. 8 c. 5                             | Perimeter entities | Notification of update of security measures                                                                   | Even if the update of the security measures does not follow the update of the list of ICT assets included in the perimeter, the perimeter entities notify the ACN. If the perimeter entities update their security measures, they notify the modalities of the update to the ACN within 6 months via its digital platform.                                                                                                                                                                                                                                                                                                                                                          | ACN                                                                                                    | 1. An update to the security measures is made without updating the list of ICT assets included in the perimeter<br>2. The modalities of the update of the security measures are notified to the ACN via its digital platform by the perimeter entity within 6 six month from the completion of the implementation |
| D.P.C.M. 81 art. 9                                  | Perimeter entities | Implementation of minimum security measures for information protection (Annex C)                              | The perimeter entities implement the minimum security measures for information protection (identified in Annex C) within 60 days from the effective date of D.P.C.M. 81. These security measures must assure the protection of the following informations:<br>a) the list of entities inside the perimeter; b) the lists of assets included in the perimeter, including the description of the architecture and components, as well as the risk analysis; (c) to the elements of the notifications of the incidents, including the additional follow-up information; d) the model and the documentation prepared in implementation of the security measures referred to in Annex B. |                                                                                                        | 1. The minimum security measures are implemented by the perimeter entities within 60 days from the effective date of D.P.C.M. 81                                                                                                                                                                                  |
| D.P.C.M. 81 art. 9 c. 4 and art. 42 L. 124 of 2007  | Perimeter entities | Application of security measures for classified information                                                   | If a security classification is applied, the perimeter entities must still comply with the security measures in l. 124 of 2007.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                        | 1. The perimeter entity processes classified information<br>2. Security measures from art. 42 L. 124 of 2007 are implemented by the perimeter entity                                                                                                                                                              |

|                                                        |                                                                                          |                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------------------|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| D.P.R. 54 art. 3 c. 5                                  | CVCN                                                                                     | Methodologies for the preparation of the risk analysis document and for the identification of test severity levels | The CVCN defines the methodologies for the preparation of the risk analysis document and for the identification of test severity levels, within 60 days from the effective date of D.P.R. 54.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Perimeter entities                                                                                                                                                                                                                                               | 1. The methodologies for the preparation of the risk analysis document and for the identification of test severity levels are defined by the CVCN, within 60 days from the effective date of D.P.R. 54                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| D.P.R. 54 art. 3 c. 4                                  | Perimeter entities                                                                       | Analysis of the relative risk associated with the object of supply                                                 | Before proceeding with the tender procedures or with the conclusion of contracts for the supply of ICT goods, systems, and services, intended to be used on perimeter assets and belonging to the categories identified by the DPCM June 15, 2021, the perimeter entities must draw up a special document for the analysis of the associated risk must be drawn up. The document shall contain a description of the following elements:<br>a) the operational environment of the area of use specifying: 1) the components with which the object of supply interacts and the configurations of these components; 2) any existing physical, technical, procedural, personnel-related security measures with an indication of any certifications or verifications performed; b) the security requirements that characterize the use of the object of supply, expressed in terms of its ability to protect the availability, integrity and confidentiality of information and services.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | The National Evaluation and Certification Centre (in Italian Centro di Valutazione e di Certificazione Nazionale or CVCN) or the evaluation centres of the Ministry of the Interior and the Ministry of Defence (in Italian simply Centri di Valutazione or CVs) | 1. A perimeter entity needs to proceed with a supply of ICT goods, systems, and services<br>2. The ICT goods, systems, and services need to be used on perimeter assets<br>3. These assets belong to the categories identified by the DPCM June 15, 2021                                                                                                                                                                                                                                                                                                                                                                                          |
| D.P.R. 54 art. 3 cc. 1-3 and D.P.R. 54 art. 10 cc. 1-2 | Perimeter entities (with the exception of public security authorities and police forces) | Notice of tender                                                                                                   | Before proceeding with the tender procedures or with the conclusion of contracts for the supply of ICT goods, systems, and services, intended to be used on perimeter assets and belonging to the categories identified by the DPCM June 15, 2021, the perimeter entities must notify the CVCN or the CVs. The communication must include the identification data of the perimeter entity and: a) the general description of the object of the supply; b) the intended use of the object of the supply within the ICT assets; c) the category to which the object of the supply belongs; d) the information and services that the object of the supply is to deal with and the related management methods; e) information on the possible acquisition through the tools referred to in Article 1, paragraph 512, of Law No. 208 of December 28, 2015. The risk analysis document associated with the object of the supply must be attached to the communication. The communication should not be made if it is indispensable to proceed with foreign procurement for the supply of the following ICT goods, systems and services. It is considered essential to proceed with foreign procurement if the supplies are for: a) implementation and upgrading of computer and telecommunications networks; b) connectivity services; and c) management, support and maintenance services for computer, network and telecommunications equipment and systems, delivered in-person at the foreign location. | CVCN or CV                                                                                                                                                                                                                                                       | 1. The perimeter entity does not belong to the public security authorities and police forces<br>2. The ICT goods, services and systems belong to the categories categories identified by the DPCM June 15, 2021<br>2. It is not indispensable to proceed with foreign procurement for the supplies of ICT goods, systems and services<br>3. The risk analysis document associated with the object of the supply is attached to the notification to the CVCN or to the CVs<br>4. The CVCN or the CVs are notified of the procurement procedures concerning the supply of ICT goods, systems, and services, intended to be used on perimeter assets |
| D.P.R. 54 art. 3 cc. 1-3                               | CVCN                                                                                     | Methodologies for preparing the risk analysis document and identifying test severity levels                        | The CVCN defines the methodologies for preparing the risk analysis document and identifying test severity levels within 60 days after the regulations come into force                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Perimeter entities                                                                                                                                                                                                                                               | 1. The methodologies for preparing the risk analysis document and identifying test severity levels are defined by the CVCN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

|                                       |                    |                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                    |                                                                                                                                                                                                                                                                                                            |
|---------------------------------------|--------------------|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| D.P.R. 54 art. 4 c. 8                 | CVCN               | Testing methodologies                                          | The CVCN shares testing methodologies with CVs and LAPs. Methodologies for conducting tests are kept strictly confidential.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | CVCN, CV or LAP    | <ol style="list-style-type: none"> <li>1. Testing methodologies are defined by CVCN</li> <li>2. Testing methodologies are shared with CVs and LAPs</li> <li>3. The methodologies are kept strictly confidential</li> </ol>                                                                                 |
| D.P.R. 54 art. 5 c. 4                 | CVCN               | Definition of tests corresponding to severity levels           | The CVCN defines the tests corresponding to the levels of severity, within 60 days of the entry into force of the regulation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Perimeter entities | <ol style="list-style-type: none"> <li>1. The tests corresponding to the levels of severity are defined by CVCN, within 60 days of the entry into force of the regulation</li> </ol>                                                                                                                       |
| D.P.R. 54 art. 5 c. 1                 | Perimeter entities | Information needed for preliminary verifications               | <p>At the request of the CVCN or a CV, the perimeter entities provide the necessary information to ensure cooperation in identifying the conditions for the supplier and the type of hardware and software testing to be performed.</p> <p>If information is incomplete or inconsistent, the terms of the procedures can be suspended for one time until complete and consistent information is provided.</p>                                                                                                                                                                                                                                                                                                                                                                                                              | CVCN or CV         | <ol style="list-style-type: none"> <li>1. Necessary information for identifying the conditions for the supplier and the type of hardware and software testing to be performed are shared by the perimeter entity with the CVCN or the CV</li> <li>2. The information is complete and consistent</li> </ol> |
| D.P.R. 54 art. 5 c. 5                 | Suppliers          | Activities preparatory to the execution of the tests           | If the CVCN or a CV requires certain tests to be performed, the supplier must perform the following preliminary activities: a) provide evidence of the suitability of the safety functions and their configurations to meet the safety requirements of Article 3(4)(b); b) provide for the setting up of a test environment adequately representative of the operational reality at the laboratory or, if necessary, at the supplier's or perimeter entity's premises; c) provide a general description of the architecture of the evaluation object and its functions; d) provide a description of the security features implemented in the evaluation object; e) provide a description of the functional and security tests already performed by the supplier or manufacturer or a third party, including their results. | CVCN or CV         | <ol style="list-style-type: none"> <li>1. The CVCN or a CV requires certain tests to be performed</li> <li>2. The preliminary activities are performed before the test by the supplier</li> </ol>                                                                                                          |
| D.P.R. 54 art. 4 c. 3                 | Suppliers          | Test execution                                                 | If the CVCN or a CV prescribes certain tests to be performed as part of pre-testing phase, the supplier must perform them.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | CVCN or CV         | <ol style="list-style-type: none"> <li>1. Tests are prescribed by the CVCN or by a CV as a part of the pre-testing phase</li> <li>2. The tests are executed by the supplier</li> </ol>                                                                                                                     |
| D.P.R. 54 art. 4 c. 3                 | CVCN or CV         | Conditions and tests for the tender notice or for the contract | When the verification procedure is completed, the CVCN or a CV defines, if necessary, conditions and tests of hardware and software to be included in the clauses of the tender notice or in contract. The conditions condition suspensively or resolutely the contract.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Perimeter entities | <ol style="list-style-type: none"> <li>1. The verification procedure is completed</li> <li>2. Conditions and tests of hardware and software are defined by the CVCN or by a CV</li> <li>3. The identified prescriptions are included in the clauses of the tender notice or in the contract</li> </ol>     |
| D.P.R. 54 art. 4 c. 3                 | CVCN or CV         | Usage requirements                                             | <p>When the identified tests are executed, the CVCN or a CV defines, if necessary, usage requirements for the test object.</p> <p>The perimeter entity must observe these possible requirement while using the object of the supply.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Perimeter entities | <ol style="list-style-type: none"> <li>1. The test phase is completed</li> <li>2. Usage requirements are observed by the perimeter entity</li> </ol>                                                                                                                                                       |
| D.P.R. 54 art. 4 c. 4 and art. 5 c. 6 | CVCN or CV         | Conclusion of preliminary verifications                        | <p>Within 45 days of the notice of tender by the perimeter entity, the CVCN or the CVs must complete the preliminary verifications.</p> <p>An additional extension of 15 days is possible for the following cases of particular complexity: a) the evaluation object consists of ICT assets, systems, and services integrated with each other; b) the evaluation object is</p>                                                                                                                                                                                                                                                                                                                                                                                                                                             | Perimeter entities | <ol style="list-style-type: none"> <li>1. The preliminary verification is completed by the CVCN or by a CV withing 45 days from the notice of tender</li> </ol>                                                                                                                                            |

|                                                 |                           |                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                          |                                                                                                                                                                                                                                                                   |
|-------------------------------------------------|---------------------------|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                 |                           |                                                              | based on newly developed technologies for which established test methodologies are not available; c) the evaluation object interacts with components that deliver other essential functions or services.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                          |                                                                                                                                                                                                                                                                   |
| D.P.R. 54 art. 5 c. 8                           | Perimeter entities        | Indication of the security requirements of the supply object | The perimeter entity conducting a tender procedure or entering into a contract, either directly or through central purchasing bodies, must indicate the security requirements of the object of supply, taking appropriate confidentiality precautions. The perimeter entity must consider possible prescriptions identified by the CVCN or by the CV.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Supplier and central purchasing agency, if any                           | 1. Security requirements for the object of the supply are indicated by the perimeter entity<br>2. The possible prescriptions of the CVCN or of the CVs are considered<br>3. Confidentiality precautions are taken by the perimeter entity                         |
| D.P.R. 54 art. 5 c. 7                           | Central purchasing bodies | Compliance with the provisions of D.P.R. 54                  | Central purchasing bodies must apply the provisions of D.P.R. 54 with reference to the procurement of ICT goods, systems and services intended for use on perimeter assets and belonging to the categories identified by the Prime Minister's Decree of June 15, 2021.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                          | 1. Provisions of D.P.R. 54 are applied by the central purchasing bodies                                                                                                                                                                                           |
| D.P.R. 54 art. 5 c. 9                           | Perimeter entities        | Disclosure of supplier and supply references                 | Once the tender award has been made or the contract has been concluded, the perimeter entity must notify the CVCN or CVs of the supplier's references and any useful element to uniquely identify the supply object.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | CVCN or CV                                                               | 1. The tender award has been made or the contract has been concluded<br>2. The supplier's references and any useful element to uniquely identify the supply object are notified to the supplier                                                                   |
| D.P.R. 54 art. 6 c. 6                           | ACN                       | Development of the IT platform to support the CVCN and CVs   | ACN develops and maintains platform to support CVCN and CVs to verify and identify previous tests carried out on a test object.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | CVCN or CV                                                               | 1. The platform to support CVCN and CVs activities is developed and maintained by the ACN                                                                                                                                                                         |
| D.P.R. 54 art. 6 c. 1                           | CVCN or CV                | Verification of previous tests                               | When the CVCN or a CV receives references from a supplier and a supply, it verifies whether that supply has already undergone security assessments or if there are controls in place.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                          | 1. The existence of previous tests on the same object is verified by the CVCN or by a CV                                                                                                                                                                          |
| D.P.R. 54 art. 6 cc. 2,3                        | CVCN or CV                | Additional tests                                             | If previous tests have been already executed, the CVCN or a CV must assess the need for additional tests. If that object has already undergone security assessments or controls, the CVCN or a CV must verify if previous activities are sufficient. Previous tests are sufficient when: a) implementation tests and intrusion tests have been performed on all security functions necessary to meet security requirements; b) intrusion tests have been performed for the same or higher severity levels than those selected. Therefore, additional tests are needed if: a) implementation tests and intrusion tests have not been performed on all security functions necessary to meet security requirements; b) intrusion tests have been performed for lower severity levels than those selected. If part of these required tests have been executed, the CVCN or a CV must indicate new supplementary tests, excluding already executed ones. | Perimeter entities                                                       | 1. Previous tests have been executed<br>2. The need for additional tests is assessed by the CVCN or by a CV<br>3. Possible additional test are identified assessed by the CVCN or by a CV                                                                         |
| D.P.R. 54 art. 6 c. 4 and D.P.R. 54 art. 7 c. 3 | CVCN or CV                | Tests identification                                         | If previous tests have not been already executed, the CVCN or a CV must identify the tests to be executed and the place for the activities. The CVCN or a CV can execute the tests directly in their laboratories or they can appoint a LAD for the execution. If necessary, the tests can be also executed at the supplier's facilities or at the perimeter entity facilities by CVCN or CV's personnel.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Perimeter entities, LAP (if appointed for the tests execution), supplier | 1. Previous tests have not been executed<br>2. The tests to be executed are identified by the CVCN or a CV<br>3. The place for the execution of the tests is identified<br>4. A LAD can be appointed for the execution of the tests on behalf of the CVCN or a CV |



|                                                 |                                                               |                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                          |                                                                                                                                                                                                                                                             |
|-------------------------------------------------|---------------------------------------------------------------|----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| D.P.R. 54 art. 6 cc. 2,5                        | CVCN or CV                                                    | Notification of completion of test preparation phase                       | If previous tests are sufficient, the CVCN or a CV notify the conclusion of the procedure to the perimeter entity and the supplier. If necessary, the CVCN or a CV can still identify usage prescriptions.                                                                                                                                                                                                                                         | Perimeter entities and suppliers                                         | 1. Previous tests are sufficient<br>2. The conclusion of the procedure is notified to the perimeter entity and the supplier by the CVCN or a CV<br>3. Possible usage prescriptions are identified by the CVCN or a CV                                       |
| D.P.R. 54 art. 7 cc. 1,2                        | CVCN or CV                                                    | Notification of start of testing                                           | The CVCN or a CV notifies the start of testing to the perimeter entity and to the supplier. The notice must specifies possible arrangements for collaboration with suppliers during the execution of the tests.                                                                                                                                                                                                                                    | Perimeter entities and suppliers                                         |                                                                                                                                                                                                                                                             |
| D.P.R. 54 art. 7 c. 3                           | CVCN or CV or LAP                                             | Execution of the identified tests                                          | CVCN, a CV or an appointed LAP execute the tests. The testing must be completed within 60 days from the date the perimeter entity makes the test object available. Where possible, tests are performed at the CVCN, a CV or LAP, otherwise at the perimeter entity or a supplier.                                                                                                                                                                  |                                                                          | 1. Identified tests are executed, within 60 days from the date the perimeter entity makes the test object available                                                                                                                                         |
| D.P.R. 54 art. 7 cc. 5,8                        | CVCN or CV or LAP                                             | Notification of malfunction                                                | In case of malfunction of the evaluation object or the test environment prepared by the supplier, the CVCN or a CV notify the perimeter entity and the supplier of the reasons that prevent from the continuation of testing. If the test is executed by a LAD, the LAD notifies the reasons to the CVCN. The 60 period for execution can be suspended for a maximum of 10 days, during which the supplier may arrange to resolve the malfunction. | Perimeter entities and providers (and CVCN if the appointee was the LAP) | 1. A malfunction of the test object or of the test environment, prevent from the continuation of the testing<br>2. The malfunction is notified to the perimeter entity and the supplier                                                                     |
| D.P.R. 54 art. 7 c. 5                           | Suppliers                                                     | Troubleshooting                                                            | After receiving the notice of the malfunction, the supplier can try to solve it within 10 days.                                                                                                                                                                                                                                                                                                                                                    | CVCN or CV                                                               | 1. The malfunction is solved within 10 days from the notice                                                                                                                                                                                                 |
| D.P.R. 54 art. 7 c. 5                           | CVCN or CV                                                    | Notification of termination of the test execution phase due to malfunction | If the malfunction cannot be resolved within 10 days from the notice, the CVCN, a CV or a LAD notify the impossibility to complete the execution of the tests to the perimeter entity and the supplier.                                                                                                                                                                                                                                            | Perimeter entities and suppliers                                         | 1. The malfunction is not solved within 10 days from the notice<br>2. The impossibility to complete the tests is notified to the perimeter entity and the supplier by the notice, the CVCN, a CV or a LAD                                                   |
| D.P.R. 54 art. 7 c. 6                           | CVCN or CV or LAP                                             | Test report                                                                | The CVCN, a CV or a LAD prepares the test report, detailing the test environment, tests performed and outcomes.                                                                                                                                                                                                                                                                                                                                    | (CVCN, if the appointee was the LAP)                                     | 1. The test report is prepared by the CVCN, a CV or a LAD                                                                                                                                                                                                   |
| D.P.R. 54 art. 4 c. 5 and D.P.R. 54 art. 8 c. 1 | CVCN or CV                                                    | Evaluation report                                                          | Within 60 days from the perimeter entity's notification of making the evaluation object available, the CVCN or a CV prepare an appropriate evaluation report and notify it to the perimeter entity and the supplier. The evaluation report is prepared considering the test report.                                                                                                                                                                | Perimeter entities and suppliers                                         | 1. The evaluation report is prepared by the CVCN or a CV, within 60 from the perimeter entity's notification of making the evaluation object available<br>2. The evaluation report is notified to the perimeter entity and the supplier by the CVCN or a CV |
| D.P.R. 54 art. 8 c. 1-3                         | CVCN or CV                                                    | Notification of the final decision of the evaluation process               | The CVCN or a CV notify an explained final decision to the perimeter entity and the supplier. The decision can be negative or positive. If the decision is positive, the CVCN or a CV can still impose prescriptions for the use of the object of reliance.                                                                                                                                                                                        | Perimeter entities and suppliers                                         | 1. A final decision about the testing procedure is taken by the CVCN or a CV<br>2. The decision is explained<br>3. The decision is notified to explained to the perimeter entity and the supplier                                                           |
| D.P.R. 54 art. 15 c. 1                          | ACN and specialized facilities of the police and armed forces | Designation of the competent authorities for verifications and inspections | The ACN and specialized facilities of the police and armed forces are the competent authorities designated for verifications and inspections activities. After the establishment of the ACN, the Presidency of the Council of Ministers and the Ministry of the economic development have been substituted in their role of supervision of public and private entitites.                                                                           |                                                                          |                                                                                                                                                                                                                                                             |

|                                                                             |                                                                                                                                                 |                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                             |                                                                                                                                                 |                                                                                 | The ACN is responsible for both public and private entities.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                    |
| D.P.R. 54 art. 15 c. 2                                                      | ACN and specialized facilities of the police and armed forces                                                                                   | Establishing and updating the list of personnel for inspection and verification | The competent authorities establish and update a list of personnel to be appointed for inspection and verification activities.<br>The personnel must meet the requirements of Article 42 l. 124 of 2007 to be able to handle information with security classification higher than "confidential".                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                 | 1. A list of personnel to be appointed for inspection and verification activities is established and updated by competent authorities<br>2. The list provides information about the security classification that each person is able to handle                                                                                                                                                                     |
| D.P.R. 54 art. 15 c. 3-4                                                    | ACN and specialized facilities of the police and armed forces                                                                                   | Identification of personnel in charge                                           | The competent authorities identify the personnel in charge of verifications and inspections, together with a person in charge of the procedure, according to criteria of professionalism and rotation.<br>The personnel declare the absence of conflict of interest when accepting the assignment.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | ACN or specialized facilities of the police and armed forces (in the figure of the staff in charge of the inspection or verification procedure) | 1. The personnel in charge of verifications and inspections is identified by the competent authorities<br>2. The personnel declare the absence of conflict of interest when accepting the assignment                                                                                                                                                                                                               |
| D.P.R. 54 Art. 16 c. 3, D.P.R. 54 Art. 16 c. 5-6 and D.P.R. 54 Art. 18 c. 3 | ACN or specialized facilities of the police and armed forces (in the figure of the staff in charge of the inspection or verification procedure) | Notice of initiation of verification or inspection procedure                    | The person in charge of the procedure notifies the persons to whom the procedure are addressed and those to whom the procedure may cause prejudice (Art. 7 l. 241 of 1990) of the start of the procedure, in the manner set forth in Art. 8 of l. 241 of 1990.<br>The verification process must be concluded within 120 days from the date of the notice.<br>The inspection process must conclude within 90 days from the date of the notice.<br>No less than 15 days' notice must be given regarding the inspection process. A notice must also be provided, with at least the following information: a) the dates and sites where the inspection will be conducted; b) the persons to be interviewed or their roles and responsibilities; c) the networks, information systems, and information technology services to be inspected; d) the names of assigned personnel; e) any other information relevant to the inspection. | Perimeter entities and any counterinterested parties                                                                                            | 1. The persons to whom the procedure are addressed and those to whom the procedure may cause prejudice are identified and notified of the start of the procedure in accordance with Art. 7 and Art. 8 of l. 241 of 1990<br>2. The process is completed within the deadlines<br>3. In case of an inspection process, notice is given at least 15 days in advance<br>4. The notice contains the required information |
| D.P.R. 54 art. 16 c. 4 and D.P.R. 54 art. 18 c. 6                           | Perimeter entities                                                                                                                              | Appointment of a person in charge of the process                                | Following notice of the initiation of the verification or inspection procedure by the responsible party, perimeter entities must appoint a person who possesses professionalism and expertise in cybersecurity. In case of an inspection, the name of the appointee must be communicated at least 5 days before the scheduled inspection date.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | ACN or specialized facilities of the police and armed forces (in the figure of the staff in charge of the inspection or verification procedure) | 1. The notice of the initiation of the verification or inspection procedure is issued by the responsible party and is received by the perimeter entities<br>2. A person who possesses professionalism and expertise in cybersecurity is appointed by the perimeter entity for the verification or inspection procedure                                                                                             |
| D.P.R. 54 art. 17 c. 2                                                      | Perimeter entities                                                                                                                              | Making available the necessary information and documentation                    | Following the notice of the initiation of the verification procedure by the person in charge of the procedure, the perimeter entities make available the necessary information and documentation within 15 days from the request.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | ACN or specialized facilities of the police and armed forces (in the figure of the staff in charge of the inspection or verification procedure) | 1. The notice of the initiation of the verification procedure is issued by the responsible party and is received by the perimeter entities<br>2. The information and documentation provided by the perimeter entities are relevant, complete, accurate, and timely, and are delivered within 15 days from the request                                                                                              |
| D.P.R. 54 art. 17 c. 3                                                      | Perimeter entities                                                                                                                              | Return of clarifications and additions                                          | Following the request by the person in charge of the procedure, the perimeter entities respond to requests for clarifications and additions within 10 days of the request.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | ACN or specialized facilities of the police and armed forces (in the figure of the staff in charge of the inspection or verification procedure) | 1. The request by the person in charge of the procedure is issued<br>2. The responses by the perimeter entities are relevant, complete, accurate, and timely, and are delivered within 10 days of the request                                                                                                                                                                                                      |

|                                                     |                                                                                                                                                 |                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| D.P.R. 54 art. 17 c. 4-5 and D.P.R. 54 art. 16 c. 7 | ACN or specialized facilities of the police and armed forces (in the figure of the staff in charge of the inspection or verification procedure) | Formation of the record of verification activities                        | The staff in charge of the procedure draws up the minutes of the activity carried out in the course of the checks and forwards it to the person in charge of the procedure.<br>If evidence is found that may constitute violations of regulatory provisions falling within the institutional responsibilities of other Administrations, the staff in charge must account for it in the report, and the competent authority must forward the relevant documentation to the competent Administrations without delay. The competent authorities can formulate specific prescriptions which perimeter entities must comply with. | ACN or specialized facilities of the police and armed forces (in the figure of the person in charge of the procedure) and competent administrations with respect to the violation of other regulatory provisions (if they have been detected)                                                   | 1. The minutes of the activity carried out in the course of the checks are drawn up by the staff in charge of the procedure<br>2. The minutes are forwarded to the person in charge of the procedure<br>3. If evidence that may constitute violations of regulatory provisions falling within the institutional responsibilities of other Administrations is found, the competent authority forwards the must forward the relevant documentation to the competent Administrations without delay<br>4. Possible specific prescriptions prescriptions which perimeter entities must comply with are formulated by the competent authorities |
| D.P.R. 54 art. 18 c. 4-5                            | Perimeter entities                                                                                                                              | Acceptance or counterproposal to inspection dates                         | The perimeter entity can accept the proposed dates for the inspection or propose other dates, with a maximum postponement of 10 days. The counterproposal must come withing 5 days from the notice of initiation of the inspection procedure. In the absence of a counterproposal, the dates are considered confirmed.                                                                                                                                                                                                                                                                                                       | ACN or specialized facilities of the police and armed forces (in the figure of the person in charge of the procedure)                                                                                                                                                                           | 1. The perimeter entity proposes possible other dates for the inspection, within 5 days from the notice of initiation of the inspection procedure<br>2. The maximum possible postponement possible is 10 days                                                                                                                                                                                                                                                                                                                                                                                                                             |
| D.P.R. 54 art. 18 c. 4                              | ACN or specialized facilities of the police and armed forces (in the figure of the person in charge of the procedure)                           | Acceptance or counterproposal to inspection dates                         | Upon receipt of the counterproposal for the new dates, the inspection authority can either accept it or make a counterproposal by sending a notice at least 7 days before the scheduled inspection date. The dates of the counterproposal are considered definite, and cannot be changed.                                                                                                                                                                                                                                                                                                                                    | Perimeter entities                                                                                                                                                                                                                                                                              | 1. The notice of the counterproposal by the inspection authority, if any, is sent to the perimeter entity at least 7 days before the scheduled inspection date<br>2. The dates of the counterproposal by the inspection authority are considered definite and cannot be changed by either party                                                                                                                                                                                                                                                                                                                                           |
| D.P.R. 54 art. 18 c. 7                              | Perimeter entities                                                                                                                              | Making personnel, devices, and facilities available during the inspection | During the inspection, the perimeter entity makes available all human resources required and necessary to facilitate related activities. For example, access to premises, devices and information relevant to the inspection should be provided.                                                                                                                                                                                                                                                                                                                                                                             | ACN or specialized facilities of the police and armed forces (in the figure of the staff in charge of the procedure)                                                                                                                                                                            | 1. All necessary human resources are made available by the perimeter entity to facilitate the inspection activities<br>2. Access to the premises, devices, and relevant information required for the inspection is provided by the perimeter entity                                                                                                                                                                                                                                                                                                                                                                                       |
| D.P.R. 54 art. 18 c. 9-10                           | ACN or specialized facilities of the police and armed forces (in the figure of the staff in charge of the procedure)                            | Formation of the record of verification activities                        | The staff in charge of the procedure draws up the minutes of the activity carried out during the inspection and forwards it to the person in charge. A copy of the minutes is issued to the person in charge of the perimeter entity. If evidence is found of which may constitute violations of regulatory provisions falling within the institutional powers of other Administrations, the assigned personnel accounts for it in the minutes, and the competent authority forwards the relevant documentation to the competent Administrations without delay.                                                              | ACN or specialized facilities of the Police and Armed Forces (in the figure of the person in charge of the proceedings), perimeter entities (in the figure of the person in charge), and competent administrations with respect to the violation of other regulatory provisions (when detected) | 1. The minutes of the inspection activity are drawn up in a clear and accurate manner, and include all the relevant information and evidence collected during the inspection<br>2. The minutes of the inspection activity are forwarded to the person in charge of the procedure and the person in charge of the perimeter entity<br>3. If any evidence of violations of regulatory provisions falling within the institutional powers of other Administrations is found, the competent authority forwards the relevant documentation to the                                                                                              |



|                                        |                                                              |                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------|--------------------------------------------------------------|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                        |                                                              |                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                    | competent Administrations without delay                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| D.P.R. 54 art. 19                      | ACN or specialized facilities of the police and armed forces | Outcomes of inspection or verification activities | The competent authority adopts the provision to conclude the procedure, imparting specific requirements if necessary.<br>The measure is communicated to the perimeter entity concerned.<br>Where necessary, the procedure for the application of sanctions must be initiated.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Perimeter entities | 1. The provision to conclude the procedure is adopted by the competent authority<br>2. The measure is communicated to the perimeter entity concerned<br>3. The possible procedure for the application of sanctions is initiated                                                                                                                                                                                                                                                                                                                                                                                                   |
| D.P.C.M. 18 maggio 2022, n. 92, art. 3 | CVCN                                                         | Designation of the accreditation body of the LAP  | The accreditation body is the CVCN, which operates in accordance with the requirements of UNI CEI EN ISO/IEC 17011 'Conformity assessment - Requirements for accreditation bodies accrediting conformity assessment bodies'.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| D.P.C.M. 18 maggio 2022, n. 92, art. 4 | CVCN                                                         | Functions of the accreditation body               | The CVCN: a) accredits the testing laboratories, in possession of the requirements; b) undertakes initiatives in order to guarantee the maintenance of the quality level of the LAPs and the correct implementation of the technical determinations, the technical specifications and the drawing up of the test reports; c) establishes the test methodologies; d) supervises the activity of the LAPs; e) adopts specific technical determinations, ensuring, within its own competences, their compliance and taking care of their updating; f) supervises the connections with the LAPs and the CVs, also in order to ensure the coordination of their respective activities and to pursue the convergence and non-duplication of assessments in the presence of the same conditions and risk levels; g) draws up and periodically update the list of ICT goods, systems and services subject to assessment, for which a test report has been issued; h) manages the IT platform for storing and sharing LAPs and summary test reports. |                    | 1. General compliance with the functions listed in Article 4 is ensured (the functions are further specified in other requirements)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| D.P.C.M. 18 maggio 2022, n. 92, art. 5 | Accreditation Commission at the CVCN                         | Accreditation Commission at the CVCN              | An Accreditation Commission will be set up at the CVCN with advisory functions, consisting of a chairman appointed by the Agency and two representatives appointed by the Ministry of the Interior and the Ministry of Defence, respectively, with technical expertise in the field of process certification and information security. The CVCN provides secretarial and support services for the functioning of the Commission.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                    | 1. The Accreditation Commission is set up at the CVCN and has a clear mandate and scope of advisory functions<br>2. The chairman of the Accreditation Commission is appointed by the Agency and has the required qualifications and authority to lead the Commission<br>3. The two representatives of the Accreditation Commission are appointed by the Ministry of the Interior and the Ministry of Defence, respectively, and have the technical expertise in the field of process certification and information security<br>4. Secretarial and support services for the functioning of the Commission are provided by the CVCN |
| D.P.C.M. 18 maggio 2022, n. 92, art. 6 | Law enforcement                                              | Collaboration with law enforcement                | In order to verify the existence and compliance of the subjective requirements for the accreditation of LAPs, the CVCN may request the police to carry out the necessary checks.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | CVCN               | 1. The CVCN request police checks to to verify the subjective requirements for LAP accreditation<br>2. The appropriate checks are carried out by the police                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| D.P.C.M. 18 maggio 2022,               | CVCN                                                         | Accreditation' areas                              | The CVCN defines the areas of accreditation for the test                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | LAPs               | 1. The areas for LAPs' accreditation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

|                                        |                                                                             |                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------|-----------------------------------------------------------------------------|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| n. 92, art. 7                          |                                                                             |                                           | laboratories.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |      | are defined by CVCN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| D.P.C.M. 18 maggio 2022, n. 92, art. 8 | Public administrations and private entities based in the national territory | Objective requirements for accreditation  | Public administrations and private organisations based in the national territory can apply for accreditation. For the purpose of accreditation, the applicant must meet the following requirements: a) availability of suitable premises and resources on the national territory; b) knowledge, skills and experience necessary to perform the functions related to accreditation in accordance with the requirements specified by the CVCN; c) compliance with the criteria specified in the standards relating to the management of testing laboratories (UNI CEI EN ISO/IEC 17025) and data management (UNI CEI EN ISO/IEC 27001); d) ability to maintain over time the requirements under which it has been accredited; e) ability to implement the security measures specified by the CVCN. If the applicant is a private entity, its ability to guarantee impartiality, independence, confidentiality and objectivity is assessed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | CVCN | <p>1. The applicant is based in the national territory</p> <p>2. The applicant meet all the requirements listed in article 8</p> <p>3. The impartiality, independence, confidentiality and objectivity of the private applicant is assessed</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| D.P.C.M. 18 maggio 2022, n. 92, art. 9 | Public administrations and private entities based in the national territory | Subjective requirements for accreditation | For the purpose of the accreditation of testing laboratories, the legal representative of the testing laboratory, the person in charge of the testing laboratory, the person in charge of the quality management system, the person in charge of relations with the CVCN, the person in charge of safety and the personnel involved in carrying out the activities for which the testing laboratory may be accredited must be of Italian nationality. None of them may be in one of the following situations: a) state of disqualification, incapacitation, bankruptcy; b) conviction, even if not final, of one of the offences identified in Article 9; c) existence of grounds for disqualification, suspension or prohibition and of an attempt of mafia infiltration. The entity must not be subject to administrative sanctions for administrative offences that are dependent on crime (d.lgs. 231/2001). The accreditation cannot be granted to a laboratory that: a) is directly involved in the design, manufacture, construction, marketing, installation, use or maintenance of ICT goods, systems or services, or whose managers or staff are the designer, manufacturer, supplier, installer, buyer, owner, authorized representative or user of the same ICT goods, systems or services; b) belongs to a business association or a professional federation that represents businesses involved in the design, manufacture, supply of ICT goods, systems or services; c) exercises control, direct or indirect, jointly or individually, over a subject or an association of businesses or a professional federation that represents businesses involved in the design, manufacture, supply of ICT goods, systems or services; d) is subject to control, direct or indirect, jointly or individually, by another subject, single or part of a consortium, that represents businesses involved in the design, manufacture, supply of ICT goods, systems or services; e) is subject to control, direct or indirect, jointly or individually, by a subject that in turn controls, directly or indirectly and/or jointly, another participant, single or part of a consortium, involved in the design, manufacture, supply of ICT goods, systems or services. | CVCN | <p>1. All the personnel of the applicant laboratory in charge of the identified roles is of Italian nationality</p> <p>2. All the personnel in charge of the identified roles is not in one of the following situations: a) state of disqualification, incapacitation, bankruptcy; b) conviction, even if not final, of one of the offences identified in Article 9; c) existence of grounds for disqualification, suspension or prohibition and of an attempt of mafia infiltration</p> <p>3. The applicant entity is not subject to administrative sanctions for administrative offences that are dependent on crime (d.lgs. 231/2001)</p> <p>4. The applicant laboratory is not directly or indirectly involved in the design, manufacture, construction, marketing, installation, use or maintenance of ICT goods</p> <p>5. There are no obstacles related to the security of the Republic</p> <p>6. The private applicant laboratory is not directly or indirectly controlled by foreign persons or entities</p> |

|                                                             |                                                                             |                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------|-----------------------------------------------------------------------------|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                             |                                                                             |                                                    | The limitations regarding the impartiality of the laboratory do not apply to test laboratories owned by a perimeter entity.<br>In any case, accreditation is not permitted if there are any reasons to impede the security of the Republic. To exclude this, private applicants must not be directly or indirectly controlled by foreign persons or entities, including through the provision of funding.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| D.P.C.M. 18 maggio 2022, n. 92, art. 10,11                  | Public administrations and private entities based in the national territory | Application for Accreditation                      | The application for is signed with a qualified electronic signature and sent to the CVCN by certified e-mail or other qualified certified electronic delivery service, accompanied by the elements listed in Articles 10 and 11 for private and public entities respectively. If the owner of the testing laboratory is a private entity, the application is signed by the legal representative. If it is a public administration, the responsible manager signs.                                                                                                                                                                                                                                                                                                                                                                                            | CVCN                                          | 1. The application for accreditation is signed with a qualified electronic signature by the legal representative of the private entity, or by the responsible manager of the pu<br>2. The application for accreditation is sent to the CVCN by certified e-mail or other qualified certified electronic delivery service<br>3. The application for accreditation is accompanied by the elements listed in Articles 10 and 11 for private and public entities respectively                                                                                                                                     |
| D.P.C.M. 18 maggio 2022, n. 92, art. 12 c. 1 let. a) n. 1-3 | CVCN                                                                        | Verification of the requirements for accreditation | The CVCN verifies the existence of the objective and subjective requirements for accreditation. In the event that the documentation is incomplete, the CVCN notifies the test laboratory and assigns it a deadline to make any additions. In the event that the test laboratory does not provide feedback within this period or in the event of continued incompleteness of the documentation, the CVCN will notify the applicant of the reasons preventing the application from being accepted. If the completeness check of the documentation is positive, the CVCN sends the applicant a list of the tests corresponding to the scope(s) of accreditation indicated in the application and requests, giving a deadline for compliance, confirming the ability to perform all or part of these tests and indicating how the testing laboratory will do so. | Applicant laboratory                          | 1. The application meets the objective and subjective requirements<br>2. If the documentation is incomplete, a deadline for addition is assigned to the test laboratory<br>3. If the check is negative the applicant is notified of the reasons preventing the application from being accepted by the CVCN<br>4. If the check is positive, a list of the tests corresponding to the scope(s) of accreditation indicated in the application and requests is assigned to the applicant laboratory to assess its ability to perform them and how<br>5. A deadline is given to the applicant laboratory to answer |
| D.P.C.M. 18 maggio 2022, n. 92, art. 12 c. 1 let. a) n. 2   | Applicant laboratory                                                        | Integration of the application                     | The applicant laboratory completes missing information in the accreditation application at the request of the CVCN.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | CVCN                                          | 1. Missing information are timely completed by the applicant laboratory                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| D.P.C.M. 18 maggio 2022, n. 92, art. 12 c. 1 let. a) n. 3   | Applicant laboratory                                                        | Definition of test capacity                        | The requesting laboratory responds to the CVCN indicating its testing capabilities in relation to the test list received.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | CVCN                                          | 1. The testing capabilities of the requesting laboratory are specified                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| D.P.C.M. 18 maggio 2022, n. 92, art. 12 c. 1 let. a) n. 4   | CVCN                                                                        | Assignment for verification activities             | After receiving feedback from the applicant, the CVCN assigns the task of reviewing the technical documentation and inspecting the applicant laboratory to Agency staff with specific technical expertise in the field of process certification and IT security.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Staff in charge of the verification procedure | 1. Agency staff with specific technical expertise in the field of process certification and IT security is appointed for reviewing the technical documentation and inspecting the laboratory                                                                                                                                                                                                                                                                                                                                                                                                                  |
| D.P.C.M. 18 maggio 2022, n. 92, art. 12 c. 1 let. b) n. 1   | Staff in charge of the verification procedure                               | Verification of technical documentation            | The responsible personnel examine the quality manual and the technical documentation and send the audit report with the results of the activities carried out to the CVCN.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | CVCN                                          | 1. The quality manual and the technical documentation are examined<br>2. The audit report with the results is sent to the CVCN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| D.P.C.M. 18 maggio 2022,                                    | CVCN                                                                        | Verification of technical                          | If the CVCN considers additions to the manual or technical documents to be necessary, it gives the                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Applicant laboratory                          | 1. If the manual or technical documents need additions, a deadline is                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

|                                                             |                                               |                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                               |                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------|-----------------------------------------------|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| n. 92, art. 12 c. 1 let. b) n. 2,3                          |                                               | documentation                           | laboratory a time limit to make the changes. In the event that the test laboratory does not provide feedback within this period or in the event of continued incompleteness of the documentation, the CVCN will notify the applicant of the reasons preventing the application from being accepted.<br>In the event of a positive outcome of the verification of the documentation, the CVCN notifies the testing laboratory and at the same time provides instructions for carrying out the inspection visit at the testing laboratory's premises. The purpose of the inspection is to verify the actual compliance with the requirements and the ability of the laboratory to perform the tests for which it has applied for accreditation. |                                                               | assigned to the test laboratory<br>2. If the check is negative, the applicant is notified of the reasons preventing the application from being accepted by the CVCN<br>3. If the check is positive, the CVCN notifies the testing laboratory<br>4. Instructions for carrying out the inspection visit at the testing laboratory's premises are provided to the applicant laboratory |
| D.P.C.M. 18 maggio 2022, n. 92, art. 12 c. 1 let. c) n. 1   | Staff in charge of the verification procedure | Inspection of the laboratory's premises | The personnel in charge of the inspection of the test laboratory request the laboratory to carry out one or more tests and to prepare the corresponding test report.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Applicant laboratory                                          | 1. The tests to be performed by the applicant laboratory are indicated<br>2. The test report for the tests is prepared                                                                                                                                                                                                                                                              |
| D.P.C.M. 18 maggio 2022, n. 92, art. 12 c. 1 let. c) n. 1   | Applicant laboratory                          | Inspection of the laboratory's premises | The applicant laboratory performs the assigned tests during the inspection and prepares the test report.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Staff in charge of the verification procedure                 | 1. The assigned tests are performed during the inspection<br>2. The test report for the tests is prepared                                                                                                                                                                                                                                                                           |
| D.P.C.M. 18 maggio 2022, n. 92, art. 12 c. 1 let. c) n. 2,3 | Staff in charge of the verification procedure | Inspection of the laboratory's premises | At the end of the inspection visit, the personnel responsible draw up a report which is signed by the legal representative of the test laboratory, the person in charge of the test laboratory and the person responsible for the quality management system. A copy of the report must always be given to the legal representative of the test laboratory. The personnel in charge of the inspection send the report to the CVCN, together with all the documents produced or acquired during the activities carried out.                                                                                                                                                                                                                     | CVCN and the legal representative of the applicant laboratory | 1. A report of the inspection is prepared<br>2. A copy of the report is given to the legal representative of the test laboratory<br>3. The minutes of the inspection are sent to the CVCN, together with all the documents produced or acquired during the activities carried out                                                                                                   |
| D.P.C.M. 18 maggio 2022, n. 92, art. 12 c. 1 let. c) n. 4   | CVCN                                          | Inspection of the laboratory's premises | If, on the basis of the minutes, the CVCN assesses the technical capacity of the test laboratory with a negative result, the CVCN communicates the reasons for the rejection of the application.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Applicant laboratory                                          | 1. If the technical capacity of the test laboratory is insufficient, explained reasons of the rejection of the application is notified by the CVCN                                                                                                                                                                                                                                  |
| D.P.C.M. 18 maggio 2022, n. 92, art. 12 c. 1 let. d) n. 1   | CVCN                                          | Opinion of the Accreditation Commission | At the end of the verification phases, the CVCN forwards to the Accreditation Commission all the documents relating to the application submitted and the verifications carried out.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Accreditation Commission at the CVCN                          | 1. All the documents relating to the application submitted and the verifications carried out are forwarded to the Accreditation Commission                                                                                                                                                                                                                                          |
| D.P.C.M. 18 maggio 2022, n. 92, art. 12 c. 1 let. d) n. 1   | Accreditation Commission at the CVCN          | Opinion of the Accreditation Commission | Within 30 days of receipt of the documentation, the Accreditation Commission issues an opinion on the applicant's suitability to perform the tasks covered by the accreditation and on any grounds for refusal, and forwards it to the CVCN.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | CVCN                                                          | 1. The opinion of the Accreditation Commission is issued, within 30 days of receipt of the documentation by the CVCN                                                                                                                                                                                                                                                                |
| D.P.C.M. 18 maggio 2022, n. 92, art. 12 c. 1 let. e) n. 1,2 | CVCN                                          | Granting or refusing the accreditation  | After obtaining the opinion of the Accreditation Commission, the CVCN issues to the applicant, in case of a positive evaluation, the accreditation certificate, valid for three years and renewable. In the event of a negative evaluation, the CVCN will provide the applicant laboratory with a reasoned refusal of the application.<br>The CVCN must complete the accreditation process within 180 days of receiving the accreditation application.                                                                                                                                                                                                                                                                                        | Applicant laboratory                                          | 1. In case of a positive evaluation, of the application, the accreditation certificate is issued<br>2. In case of a positive evaluation, the CVCN will provide the applicant laboratory with a reasoned refusal of the application<br>3. The whole certification procedure is completed within 180 days of receiving of the application for accreditation                           |

|                                                                                                |                                               |                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |      |                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------------------|-----------------------------------------------|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| D.P.C.M. 18 maggio 2022, n. 92, art. 13                                                        | LAP                                           | Duties of the LAPs                    | For the purposes of maintaining accreditation, LAPs are obliged to: a) operate on the basis of what is provided for in the technical determinations; b) promptly inform the CVCN of any variation concerning the information submitted in support of the application for accreditation; c) transmit the test report to the CVCN within the established deadlines; d) carry out the activities related to the accreditation exclusively at the premises located on the national territory and indicated in the application for accreditation; e) ensure adequate training of its personnel in order to comply with the non-disclosure commitment; f) inform the CVCN and the eventual LAP has processed data or systems concerning the latter, of any limitation of operations for more than 24 hours, within the following 24 hours. | CVCN | 1. Compliance with the functions listed in Article 13 is ensured                                                                                                                                                                                                                                                                                                                                                                                      |
| D.P.C.M. 18 maggio 2022, n. 92, art. 14, cc. 1-3                                               | CVCN                                          | Supervision of the activities of LAPs | The CVCN arranges for audits to be carried out periodically, at a maximum of every 18 months, to verify the maintenance of the accreditation requirements. The CVCN may carry out random inspections to verify the fulfilment of the conditions for maintaining accreditation. The CVCN, at least 2 months in advance of the scheduled date, informs the LAP of the date scheduled for the surveillance inspection, requesting any integration of the documentation in the event of any changes that have resulted in the need to revise the system documentation.                                                                                                                                                                                                                                                                   | LAPs | 1. Periodic audits are carried out at a maximum of every 18 months<br>2. Notice of the inspection is given at least 2 months in advance<br>3. Possible integration of the documentation are requested by CVCN<br>4. The appropriate personnel is appointed for the inspection                                                                                                                                                                         |
| D.P.C.M. 18 maggio 2022, n. 92, art. 14 cc. 4,5                                                | Staff in charge of the verification procedure | Periodic inspection of LAPs           | The appointed personnel verify the documentation and carry out the inspection at the LAP to assess its requirements. At the end of the inspection, the appointed personnel sends to the CVCN the verification report on the compliance of the LAP with the requirements of the accreditation scope.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | CVCN | 1. The technical documentation is verified<br>2. At the end of the inspection, the verification report is sent to the CVCN                                                                                                                                                                                                                                                                                                                            |
| D.P.C.M. 18 maggio 2022, n. 92, art. 14 cc. 6,7 and<br>D.P.C.M. 18 maggio 2022, n. 92, art. 15 | CVCN                                          | Periodic inspection of LAPs           | If the verification carried out by the appointed personnel gives a positive result, the CVCN communicates the result to the LAP. In the event of a negative result of the verification carried out by the appointed personnel, the CVCN communicates the result to the LAP and establishes, if necessary, the modalities and conditions for the rectification of the nonconformities. The CVCN, after consultation with the Accreditation Commission, requests the non-compliant LAP to take the necessary action to correct the identified nonconformities within 10 days. If the laboratory has not taken the necessary corrective action within the deadline, the accreditation is suspended. After 3 months from the date of suspension, if the nonconformities have not been corrected, the accreditation is withdrawn.         | LAPs | 1. The result of the evaluation is communicated to the LAD<br>2. In case of a negative result, necessary, the modalities and conditions for the rectification of the nonconformities are identified and communicated to the LAP<br>3. If corrective action is not taken within 10 days, the accreditation is suspended<br>4. If the nonconformities are not corrected within 3 months from the date of the suspension, the accreditation is withdrawn |
| D.P.C.M. 18 maggio 2022, n. 92, art. 16                                                        | LAPs                                          | Renewal of accreditation              | Within 6 months prior to the expiry of the accreditation certificate, the LAP may submit an application to the CVCN for renewal of the accreditation for a further three years.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | CVCN | 1. Within 6 months prior to the expiry of the accreditation certificate, an application for renewal of the accreditation is submitted                                                                                                                                                                                                                                                                                                                 |
| D.P.C.M. 18 maggio 2022, n. 92, art. 16                                                        | CVCN                                          | Renewal of accreditation              | The CVCN examines the application and arranges for an inspection to verify compliance with the accreditation requirements. If the appointed personnel give a favourable opinion, the CVCN, after consulting the Accreditation Commission, issues the certificate of renewal of accreditation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | LAPs | 1. The appropriate personnel is appointed for the inspection<br>2. The inspection is performed<br>3. In case of the favourable opinion of the personnel, the certificate of renewal of accreditation is issued                                                                                                                                                                                                                                        |



|                                         |                                                      |                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                               |                                                                                                                                                                                                                                                                 |
|-----------------------------------------|------------------------------------------------------|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                         |                                                      |                                         | If the appointed personnel does not give a favourable opinion, the CVCN communicates the result to the LAP and establishes the modalities and conditions for the elimination of the nonconformities found, if they can be eliminated. Otherwise, the CVCN, after consulting the Accreditation Commission, does not renew the accreditation.                                                                                                                                                                                               |                                                               | 4. In case of the negative opinion of the personnel, the modalities and conditions for the elimination of the nonconformities are defined<br>5. If the nonconformities are not eliminated or cannot be eliminated, the accreditation is not renewed             |
| D.P.C.M. 18 maggio 2022, n. 92, art. 20 | Ministry of the Interior and Ministry of the Defence | Application for Accreditation           | Ministries apply for accreditation of their evaluation centres by certified mail. The CV issues a declaration of compliance and informs the CVCN of: a) the address of the laboratory site where the tests are carried out; b) the general management/entity where the CV is located; c) the quality manual and the security measures implemented.                                                                                                                                                                                        | CVCN                                                          | 1. The application for accreditation is sent to the CVCN by certified e-mail<br>2. The application contains the declaration of compliance and the other contents of article 20                                                                                  |
| D.P.C.M. 18 maggio 2022, n. 92, art. 21 | CVCN                                                 | Connections between CVCN, CVs, and LAPs | The CVCN provides the appropriate connections to CV and LAP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | CVs and LAPs                                                  |                                                                                                                                                                                                                                                                 |
| D.P.C.M. 18 maggio 2022, n. 92, art. 22 | CVCN, CVs, and LAPs                                  | Incidents notification                  | The CVCN, the CVs and the LAPs notifies the CSIRT of any incident occurring on the networks, information systems and computer services related to the performance of the functions covered by the accreditation, which compromises the integrity or confidentiality of the data and information processed, within 6 hours of becoming aware of the incident. They also provide useful follow-up information about the incident, autonomously or at the request of the CSIRT, if the incident is not subject to the investigative secrecy. | CSIRT (and CVCN if the incident is notified by a CV or a LAP) | 1. Security incidents are notified to the CSIRT within 6 hours<br>2. The incident is not subject to the investigative secrecy<br>3. The incident notification is supplemented by the perimeter entity at the request of the CSIRT within 6 hours of the request |

II Appendix II – Mapping of the European legislation about cybersecurity

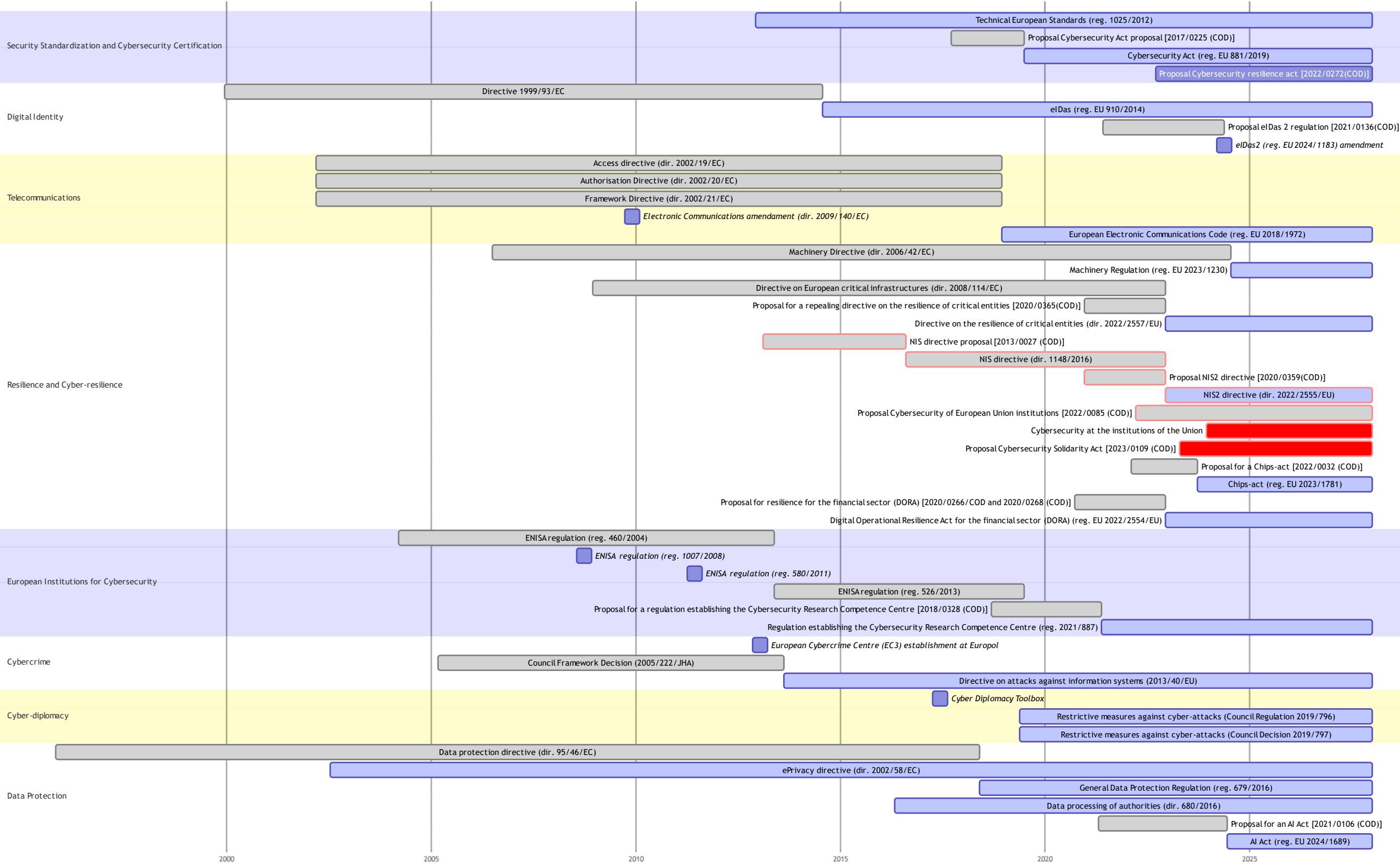


Figure 42 - Gantt chart of European legislation relevant to cybersecurity

III Appendix III – Table of main findings from European legislation

Table 2 - Main findings from European legislation

| Sector        | Source                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Key points from most relevant regulations                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | National legislation                                                                                                                  | National competent authority |
|---------------|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| Certification | Cybersecurity Act (reg. EU 881/2019)          | <p>The Cybersecurity Act strengthens the EU's cybersecurity framework by establishing a permanent mandate for ENISA, the European Union's cybersecurity agency, and creating a European cybersecurity certification framework. Key elements:</p> <p>In January 2024, the European Commission approved the first voluntary EU Cybersecurity Certification Scheme (EUCC). This scheme applies to ICT products, including hardware and software, and certifies them at the essential and high assurance levels. It sets standards for the evaluation of products such as chips and smart cards, helping to ensure a higher level of cybersecurity in the EU market. The Regulation applies across the EU, with Member States designating national cybersecurity certification authorities to enforce the rules. It will enter into force on 27 June 2019, with provisions on certification authorities and complaints coming into force on 28 June 2021.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <p>1. ENISA's mandate: ENISA supports national authorities and EU institutions in improving cybersecurity, serves as a reference point for technical advice and helps to reduce fragmentation in the internal market. It also promotes EU-wide capacity building, operational cooperation and cybersecurity certification.</p> <p>2. Cybersecurity Certification Framework: The law introduces voluntary EU-wide cybersecurity certification schemes for ICT products, services and processes, aiming to increase trust and security by assessing and certifying their cybersecurity standards. ICT products can be certified at basic, essential or high assurance levels, depending on the security requirements they meet. Certified products must include public information on the duration of security support, guidance for users and details of known vulnerabilities. ENISA designs candidate certification schemes, evaluates them every five years and maintains a portal with information on certification schemes and certificates issued.</p> | Legislative decree 3 August 2022, n. 123 and art. 7 let. e) decree law 14 June 2021, n. 82 as sanctioned by law 4 August 2021, n. 109 | ACN                          |
|               | Cybersecurity Resilience Act (2022/0272(COD)) | <p>This proposal aims to improve the EU's cybersecurity resilience by introducing mandatory cybersecurity requirements for products with digital elements. The legislation aims to improve consumer protection by making manufacturers responsible for cybersecurity throughout a product's lifecycle, including providing security updates and transparent information to users. The proposal underwent significant revisions during the legislative process. It was finally adopted by the Parliament in March 2024. The text still needs to be formally adopted by the Council before it can enter into force and is expected to be fully applicable by 2027. The latest version of the text applies to all products with digital elements placed on the market whose intended or reasonably foreseeable use involves a direct or indirect connection to a device or network. However, the Regulation only has a subordinate role, as it does not affect the application of more specific legislation, such as Regulation (EU) 2017/745 on medical devices; Regulation (EU) 2017/746 on in vitro diagnostic devices; Regulation (EU) 2019/2144 on motor vehicle safety; Regulation (EU) 2018/1139 on civil aviation safety. It also excludes spare parts that are identical to original components and products developed for national security or defence purposes. The Commission may also limit or exclude certain products where other sectoral rules provide equivalent or higher protection.</p> | <p>1. Cybersecurity obligations: Manufacturers must ensure that products are free of known vulnerabilities, include secure default configurations, and provide ongoing security support throughout the product lifecycle.</p> <p>2. Conformity assessments: Products must undergo a conformity assessment, documented in technical documentation, and comply with essential cybersecurity requirements in order to be CE marked.</p> <p>3. Post-market surveillance: Manufacturers must monitor vulnerabilities and incidents, report significant issues to ENISA within 24 hours and provide relevant updates to users.</p> <p>4. Responsibilities of economic operators: Importers and distributors must verify that products comply with cybersecurity requirements before placing them on the market, including ensuring CE marking and accompanying security information.</p>                                                                                                                                                                          | n.a.                                                                                                                                  | n.a.                         |



|                    |                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                   |                                       |
|--------------------|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|---------------------------------------|
| Digital identity   | eIDAS (reg. EU 910/2014) as amended by eIDAS2               | This regulation facilitates secure and seamless cross-border electronic identification (eID) and trust services across the EU. The eIDAS regulation enhances cybersecurity by enabling secure and trusted authentication mechanisms, thus reducing fraud and improving digital security for users and businesses. eIDAS 2 is an update to the original regulation, aiming to enhance digital identification in the EU, particularly by creating a secure European digital identity wallet. The release of the European digital identity wallet is accompanied by the introduction of specific security features. | <p>1. Security of the identity wallet: the wallet code must be open source, security by design and certified for cybersecurity in the light of the framework established by the Cybersecurity Act (Art. 5c).</p> <p>2. Security breach of the identity wallet: any breach of the wallet's security must result in users being informed (Art. 5e) and the validity of the wallet being suspended or revoked in the event of a serious breach (Art. 5a).</p> <p>3. Interoperability of identity wallet: the new European electronic wallet should be accepted by all European public service providers as a means of electronic identification (Art. 5d).</p> <p>4. Security breach of the electronic identification system: the same security breach procedure is also foreseen in the event of a breach of the security of electronic identification systems (Art. 10), which in turn must be certified for cybersecurity (Art. 12a).</p> <p>5. Cybersecurity requirements for trust services: cybersecurity also becomes an essential and explicit requirement for trust services, both qualified and unqualified (Art. 19, 24). Trust services must also notify the national authority of any data breach within 24 hours and, if necessary, the natural or legal person affected.</p> | n.a.                                                                                              | AgID                                  |
| Telecommunications | European Electronic Communications Code (dir. EU 2018/1972) | The European Electronic Communications Code updates the regulatory framework for telecom networks and services in the EU, focusing on 5G and high-capacity networks. It integrates new rules to ensure the security of electronic communication networks, mainly the mandatory obligation to implement security measures and the notification of security incidents.                                                                                                                                                                                                                                             | <p>1. Mandatory Security Measures (Art. 40): providers of public electronic communications networks and services must implement appropriate technical and organizational measures to manage risks to network security. These measures should ensure a level of security appropriate to the risk.</p> <p>2. Incident Reporting (Art. 40 par. 2): providers are obligated to notify relevant national authorities of significant security incidents that have a substantial impact on network operations. The notification must include details about the breach, its consequences, and any mitigation measures taken. The directive aims to harmonize reporting procedures across the EU to improve overall resilience.</p> <p>3. Monitoring and Testing (Art. 40 par. 3): providers must continuously monitor and test their network security. Regular assessments, audits, and logs are mandatory to detect vulnerabilities and mitigate risks in a timely manner. Providers are expected to follow recognized international security standards to ensure compliance.</p>                                                                                                                                                                                                               | Legislative decree 1 August 2003, n. 259 as amended by legislative decree 8 November 2021, n. 207 | Ministry of Economic Development, ACN |

|                                 |                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                |                                                                                                                                   |
|---------------------------------|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Resilience and Cyber-resilience | Machinery Regulation (reg. EU 2023/1230)                                               | The Machinery Regulation (MR) updates the previous directive and sets health and safety requirements for machinery, including AI-driven systems. It requires conformity assessments and introduces high-risk categories, such as machines with self-learning capabilities. The MR includes cybersecurity obligations, requiring manufacturers to protect against cyber threats and software corruption. Third-party assessments will now be required for high-risk machinery. Manufacturers must ensure compliance with health and safety standards (Annex III) and affix a CE marking. The regulation includes detailed security obligations to protect machinery from cyber threats. The regulation becomes mandatory on 20 January 2027, with no coexistence period. It aims to ensure the safe integration of machinery into the EU market, focusing on compliance, safety and security.                    | 1. Conformity assessment: listed machinery and related products in specified categories are subject to specific conformity assessment procedures (Art. 6, 25).<br>2. Health and safety requirements: machinery or related products may only be made available on the market or put into service if they meet the essential health and safety requirements listed in the regulation (Art. 8).<br>3. Certification: conformity with the essential health and safety requirements may be presumed if the product conforms to harmonised standards (Article 20).<br>Conformity with cybersecurity requirements can be presumed if the product is certified under a cybersecurity certification scheme.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | n.a.                                           | Ministry of Economic Development and Ministry of Labour                                                                           |
|                                 | Directive on the Resilience of Critical Entities (dir. EU 2022/2557)                   | The new CER Directive establishes a framework to improve the physical resilience of critical facilities across the European Union to ensure the continued provision of essential services vital to the economy and society. It addresses the growing interdependence and vulnerability of critical sectors to natural hazards, terrorism, pandemics and hybrid threats. The Directive applies to entities in 11 critical sectors, including energy, transport, health, drinking water, banking and public administration. It requires these entities to implement resilience measures against risks such as natural disasters, industrial accidents and state-sponsored threats. The Directive entered into force in December 2022 and Member States must identify critical entities by 17 July 2026. It complements the NIS2 Directive to ensure comprehensive coverage of both physical and cyber resilience. | 1. National strategies and national risk assessment: Member States must adopt national strategies (Art. 4), carry out regular risk assessments and identify critical entities (CE) (Art. 5). Support must be provided to improve resilience through guidance, training and advisory missions.<br>2. Risk assessments of Critical Entities: Critical entities must carry out their own risk assessments every four years and implement security, technical and organisational measures to safeguard their operations (Art. 12).<br>3. Incident reporting: Critical entities must report incidents that disrupt essential services within 24 hours of discovery (Art. 15).<br>4. Cross-sector support: The Directive encourages cross-border cooperation, with the Critical Entities Resilience Group (CERG) established to facilitate the exchange of best practices and information between Member States and the European Commission (Art. 19).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Legislative decree 4<br>September 2024, n. 134 | President of the Council of the Ministry and specialised sectoral authorities for the identification of the entities in the scope |
|                                 | Digital Operational Resilience Act for the financial sector (DORA) (reg. EU 2022/2554) | The DORA Regulation (EU) 2022/2554 establishes common rules to enhance the digital operational resilience of financial entities, ensuring that they can withstand, respond to and recover from ICT-related disruptions and cyber threats. It applies to a wide range of financial entities, including banks, insurance companies, payment institutions and third-party ICT service providers, such as cloud services (Art. 2). DORA is part of the EU's Digital Finance Package, which aims to strengthen the resilience of the financial sector against increasing ICT risks and cyber threats. The Regulation will apply from 17 January 2025.                                                                                                                                                                                                                                                                | 1. ICT risk management: Financial institutions must implement comprehensive ICT risk management frameworks covering risk identification, prevention, response and recovery. This includes ensuring the security of ICT systems, monitoring cyber threats and preparing business continuity plans (Art. 5-16).<br>2. Incident reporting: Financial institutions are required to classify, record and report major ICT-related incidents to their national authorities and relevant EU bodies such as the ECB and the ESAs. Where appropriate, they must inform affected customers (Art. 17-23).<br>3. Testing: Institutions must conduct regular operational resilience testing, including advanced threat-led penetration testing (TLPT) for larger institutions, to ensure that their systems can withstand cyber threats. Testing is required at least every three years for high-risk financial institutions (Art. 24-27).<br>4. Third party ICT risk: DORA introduces strict oversight of third party ICT service providers critical to the financial sector. Financial institutions must manage risks from these providers and ensure that contracts include cybersecurity and resilience clauses (Art. 28-30).<br>5. Oversight of critical ICT providers: The Regulation establishes an oversight framework in which the European Supervisory Authorities (ESAs) designate critical ICT providers and monitor their risk management capabilities (Art. 31-44).<br>6. Information sharing: Financial institutions are encouraged to share information on cyber threats and incidents within trusted communities, with safeguards for | n.a.                                           | Ministry of Economy and Finance                                                                                                   |

|  |                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                               |                                                                                                   |
|--|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|---------------------------------------------------------------------------------------------------|
|  |                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | confidentiality and data protection (Art. 45).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                               |                                                                                                   |
|  | NIS2 (dir. EU 2022/2555) | The NIS2 Directive strengthens the EU's cybersecurity framework, replacing the NIS1 Directive, and aims to harmonise cybersecurity measures across Member States. It introduces uniform cybersecurity risk management requirements and incident reporting obligations for companies operating in critical sectors. The Directive, which entered into force on 14 December 2022, must be transposed into national law by 17 October 2024, with full application from 18 October 2024. | 1. Extended scope: NIS2 extends its scope to cover a wider range of critical sectors, including energy, transport, banking, healthcare and public administration, among others, and distinguishes between Essential Entities (EE) and Important Entities (IE).<br>2. Cybersecurity risk management: Entities must implement security measures such as incident handling, supply chain security, vulnerability disclosure, encryption and multi-factor authentication (Art. 21).<br>3. Incident reporting: A two-step reporting process is introduced - initial notification within 24 hours and a final report within 72 hours for significant incidents (Art. 23). Voluntary reporting of lower-level incidents is also allowed (Art. 30).<br>4. Supervision and enforcement: EE are subject to both ex-ante and ex-post monitoring, while IE are subject to ex-post monitoring. Fines of up to €10 million or 2% of total turnover may be imposed for non-compliance (Art. 34).<br>5. Coordination and cooperation: Enhanced cooperation between Member States, including through CSIRTs, EU-CyCLONe and a structured cooperation group, ensures a consistent response to cyber incidents. | Government 17/06/2024, n. 164 | Bill ACN and specialised sectoral authorities for the identification of the entities in the scope |

|                                         |                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                       |      |
|-----------------------------------------|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|------|
|                                         | Cybersecurity Solidarity Act (2023/0109(COD))               | <p>The Cyber Solidarity Act, proposed on 18 April 2023, aims to reinforce the EU's ability to detect, prepare for, and respond to cybersecurity threats across Member States. It introduces several new initiatives designed to bolster the EU's collective cyber defenses in the face of growing and increasingly complex cybersecurity challenges.</p> <p>The text was approved by the European Parliament on 24 April 2024 and awaits formal adoption by the Council before entering into force.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <p>1. European Cyber Shield: A platform consisting of national and cross-border Security Operations Centres (SOCs) (renamed 'Cyber Hubs' in the Council's revisions), designed to improve real-time detection, analysis, and response to cyber threats across the EU.</p> <p>2. Cyber Emergency Mechanism: This mechanism enhances the EU's preparedness and response to large-scale cyber incidents by testing vulnerabilities in critical sectors; Creating an EU Cybersecurity Reserve, comprised of trusted incident response services from private providers, to assist Member States in case of significant cybersecurity incidents; Providing financial support to facilitate mutual assistance between Member States.</p> <p>3. Cybersecurity Incident Review Mechanism: A review system to assess and learn from significant or large-scale cyber incidents, improving future responses.</p> | n.a.                                                                                                                                  | n.a. |
| European Institutions for Cybersecurity | Cybersecurity Research Competence Centre (reg. EU 2021/887) | <p>The European Cyber Security Competence Centre (ECCC) and the Network of National Coordination Centres (NCCs) have been established to strengthen EU leadership in cyber security and to coordinate investments between the EU, Member States and industry. The ECCC plays a key role in the Digital Europe programme and contributes to Horizon Europe. The mission is to strengthen the EU's leadership in cybersecurity by enhancing trust, security and resilience of networks, systems and critical infrastructure. The creation of new cybersecurity capabilities can promote security by design and foster a strong European cybersecurity ecosystem through joint investments and strategic coordination. Each Member State designates an NCC to provide expertise, support cross-border projects and facilitate EU-funded cybersecurity activities. NCCs also contribute to research, education and innovation at national level. A Cybersecurity Competence Community, a network of industry, academic and public stakeholders, contributes to the ECCC by sharing expertise and contributing to cybersecurity projects.</p> | <p>1. Establishment of the ECCC and NCC Network: the regulation sets up the European Cybersecurity Competence Centre (ECCC) and a Network of National Coordination Centres (NCCs) to enhance cooperation in cybersecurity.</p> <p>2. Cybersecurity Competence Community: comprising industry, academia, research institutions, and civil society, this community contributes to the ECCC's mission by sharing and disseminating cybersecurity expertise.</p> <p>3. Governance Structure: the ECCC includes a Governing Board (representatives from Member States and the European Commission), an Executive Director responsible for daily operations, and a Strategic Advisory Group to advise on priorities.</p>                                                                                                                                                                                    | Legislative decree 3 August 2022, n. 123 and art. 7 let. e) decree law 14 June 2021, n. 82 as sanctioned by law 4 August 2021, n. 109 | ACN  |

|                 |                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                  |                                        |
|-----------------|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|----------------------------------------|
| Cybercrime      | Directive on Attacks Against Information Systems EU (2013/40) | This directive combats cybercrime by criminalizing serious cyber-attacks such as hacking and denial-of-service attacks. It promotes cooperation between law enforcement agencies and establishes consistent legal frameworks across member states, enhancing the EU's ability to combat cybercrime.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <p>1. Criminal Penalties: requires Member States to impose effective, proportionate, and dissuasive criminal penalties for cybercrimes, including intentional instigation, aiding, abetting, and attempts. The criminal offences punished in particular were illegal access to information systems, illegal system interference, illegal data interference, and illegal interception (Art. 3-6).</p> <p>2. Aggravating Circumstances: introduces harsher penalties for offences committed by organised criminal groups, or when an attack causes significant harm or involves identity theft (Art. 9).</p> <p>3. Liability of Legal Entities: establishes the responsibility of legal persons involved in cybercrimes and sets out applicable sanctions for their involvement (Art. 10).</p> <p>4. Jurisdiction Rules: requires each Member State to have jurisdiction over offences committed on its territory or by its nationals abroad, and mandates cooperation when multiple countries have jurisdiction.</p> <p>5. International Cooperation: enhances international collaboration by establishing national points of contact, using a 24/7 contact network, and responding to urgent requests within 8 hours (Art. 13).</p> | Italian Criminal Code and other sectoral sources | Judicial authorities and police forces |
| Cyber-diplomacy | Council Regulation 2019/796                                   | This regulation allows the EU to impose sanctions on individuals and entities responsible for cyber attacks, in particular those that threaten EU interests. The framework targets cyber-attacks with a significant impact, in particular those originating or supported from outside the EU. These attacks may affect critical infrastructure, essential services (e.g. energy, health, finance), government functions, classified information or emergency response teams. The framework also applies to cyber-attacks against non-EU countries or international organisations when necessary to achieve EU foreign and security policy objectives. The EU can impose travel bans and asset freezes on persons or entities responsible for, supporting or attempting cyber attacks. These sanctions also apply to persons associated with the listed persons or entities. It's a key legal tool in the EU's cyber defence, deterring cyber attacks through international legal action. | <p>1. Sanctions Framework: establishes a legal framework for the EU to impose sanctions on individuals or entities responsible for cyber-attacks, attempted attacks, or those providing support for such activities. Sanctions include travel bans to the EU and asset freezes for listed individuals or entities involved in cyber-attacks, with their details included in Annex I of Decision CFSP 2019/797.</p> <p>3. Member States' Responsibility: EU countries must define and enforce penalties for violations of these sanctions.</p> <p>4. Scope of Cyber-Attacks: targets cyber-attacks that have a significant impact, particularly those originating or supported from outside the EU, or using infrastructure located outside the EU.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | n.a.                                             | n.a.                                   |

|                 |                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                      |                   |
|-----------------|--------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| Data protection | General Data Protection Regulation (GDPR) (reg. EU 2016/679) | The GDPR regulates the processing of personal data within the EU by the private sector and most of the public sector. It gives individuals greater control over their personal data, strengthens existing rights, and introduces new ones, such as data portability and the right to erasure. GDPR applies to both EU and non-EU businesses offering services to EU citizens.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <p>1. Security of processing: Controllers and processors must implement appropriate technical and organisational measures (e.g. pseudonymisation, encryption) to ensure the confidentiality, integrity and availability of personal data. This includes ongoing monitoring and periodic evaluation of security measures (Art. 32).</p> <p>2. Notification of security breaches: Controllers must notify the relevant supervisory authority within 72 hours of becoming aware of a data breach, unless the breach is unlikely to result in a risk to the rights of individuals. In the case of high risk breaches, the individuals concerned must also be notified (Art.s 33, 34).</p> <p>3. Privacy impact assessments: Required for high-risk processing activities, especially those involving new technologies or large-scale processing of sensitive data (Art. 35).</p> <p>4. Data protection by design and by default: Organisations must build data protection into systems and processes from the earliest stages of development (Art. 25).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Legislative decree 30 June 2003, n. 196 (the so-called Italian Privacy Code) as amended by legislative decree 10 August 2018, n. 101 | DPA               |
|                 | ePrivacy Directive (dir. 2002/58/EC)                         | This directive focuses on protecting privacy in electronic communications. It complements GDPR by applying to specific sectors like telecoms and digital services, and ensures the confidentiality of communications, crucial in maintaining cybersecurity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <p>1. Confidentiality of communications: Ensure confidentiality of communications and traffic data on public networks. Technical storage necessary for communication conveyance is possible without prejudice of confidentiality (Art. 5).</p> <p>2. Data breach: Providers of electronic communications services must notify the national authority without delay in the event of a personal data breach. If the breach is likely to affect subscribers' or individuals' privacy, they must also be notified, unless the provider can prove that effective technological measures were in place to protect the data. Notifications must detail the breach, steps taken, and how individuals can mitigate any potential harm. The authority may also require providers to notify affected individuals if necessary.</p> <p>3. Access to devices storage: Access to information in terminal equipment is only allowed on condition of a clear and informed consent. Technical storage and access for the conveyance of the communication is always possible (Art. 5).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Legislative decree 30 June 2003, n. 196 (the so-called Italian Privacy Code)                                                         | DPA               |
|                 | AI Act (reg. EU 2024/1689)                                   | The Artificial Intelligence Act (AI Act) establishes a harmonised regulatory framework to ensure the safety of artificial intelligence. This legislation is part of the broader European strategy to make Europe fit for the digital age, and is in line with previous initiatives such as the European Commission's Ethics Guidelines for Trustworthy AI and the White Paper on AI. The Regulation introduces rules for AI systems, including cybersecurity measures to mitigate the risks of AI-related cyberattacks. As AI becomes an integral part of digital systems, protecting AI systems from misuse or cyber threats is essential for overall cybersecurity. In particular, it aims to regulate the development, deployment and use of artificial intelligence systems in the EU, balancing innovation with security and the protection of fundamental rights. The AI Act was adopted by the European Parliament in March 2024 and approved by the Council in May 2024. It was formally signed on 13 June 2024 and will enter into force 20 days after its publication in the Official Journal of the EU. Its provisions will be phased in over two years, with bans and compliance for high-risk | <p>1. Risk-Based Framework: it introduces a risk-based framework to address concerns related to specific AI systems, categorising them into prohibited (unacceptable risk, such as those involving subliminal manipulation or social scoring by public authorities), high risk (impacting critical areas such as biometric identification, healthcare or public services), limited risk (chatbots or deepfakes are subject to transparency requirements to ensure users are informed about the interaction with AI) and minimal risk categories (no specific requirements apply).</p> <p>2. Cybersecurity requirements: the AI Act includes specific cybersecurity obligations to ensure that high-risk AI systems are robust and secure against potential cyberattacks. Providers must implement strong security measures to mitigate threats such as unauthorised access, data manipulation and model extraction attacks. AI systems must be resilient to interference throughout their lifecycle, from development to deployment and continuous learning (Art. 15). This is one among other obligations (Art. 8-15).</p> <p>3. General-Purpose AI (GPAI) compliance: the law introduces new rules for general-purpose AI models, such as large language models, requiring providers to maintain up-to-date technical documentation and conduct risk assessments. Providers must ensure the cybersecurity of GPAI systems, especially if they are used for high-risk purposes. In addition, GPAI models that pose systemic risks must comply with risk mitigation and reporting requirements, compliance with which may be guided by codes of conduct (Art. 53).</p> <p>4. Conformity Assessments: providers of high-risk AI systems must carry out</p> | Government Bill 13 June 2024, n. 1146                                                                                                | AgID, ACN and DPA |



|  |  |                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |  |
|--|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
|  |  | <p>systems required by 2026. Meanwhile, a European Artificial Intelligence Office has been established at the European Commission in January 2024 to oversee the implementation of the AI law (Art. 64).</p> | <p>conformity assessments to ensure compliance with the Regulation. This may involve internal assessments or third party assessments, with CE marking being awarded to systems that meet the regulatory requirements. AI systems undergoing substantial modifications are also subject to new ex-ante conformity assessments (Art. 41-43).</p> <p>5. Fundamental Rights Impact Assessment: deployers of certain high-risk AI systems, particularly in sectors such as banking and insurance, must carry out fundamental rights impact assessments to ensure that the systems do not infringe individuals' rights (Art. 27).</p> <p>7. Regulatory Sandboxes: the AI Act promotes innovation through regulatory sandboxes, which allow high-risk AI systems to be tested in real-world conditions under the supervision of regulators (Art. 57).</p> <p>8. Post-market monitoring and incident reporting: providers of high-risk AI systems shall establish a post-market monitoring system (Art. 72) and report any serious incident to the market surveillance authorities when there is a causal link between the AI system and the incident (Art. 73).</p> <p>9. Penalties: failure to comply with the AI Act can result in significant penalties. Violations involving prohibited AI practices can result in fines of up to €35 million or 7% of annual global turnover (Art. 99).</p> |  |  |
|--|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|



IV Appendix – Key sources of national law for the National Cybersecurity Perimeter

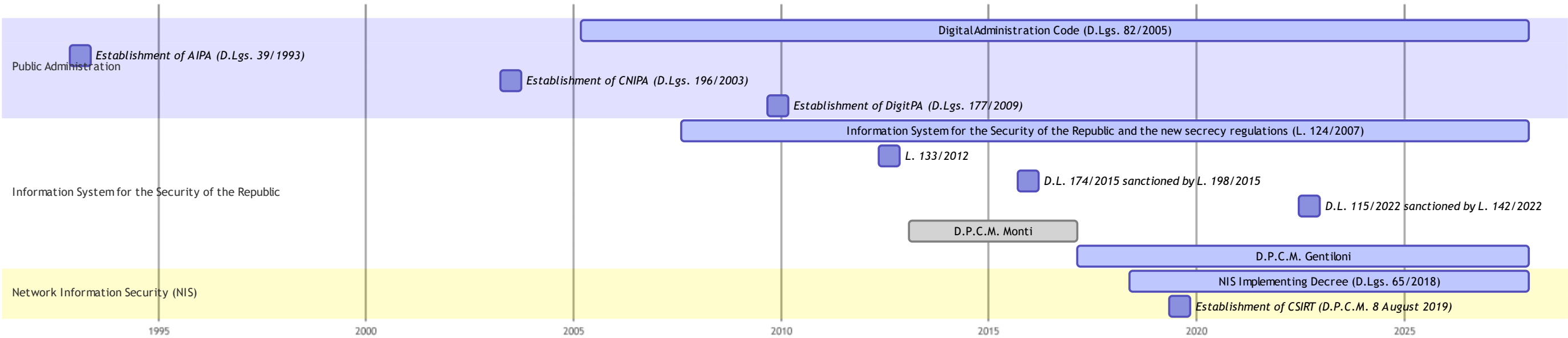


Figure 43 - Sources of the Italian Cybersecurity Framework before the establishment of the National Cybersecurity Perimeter

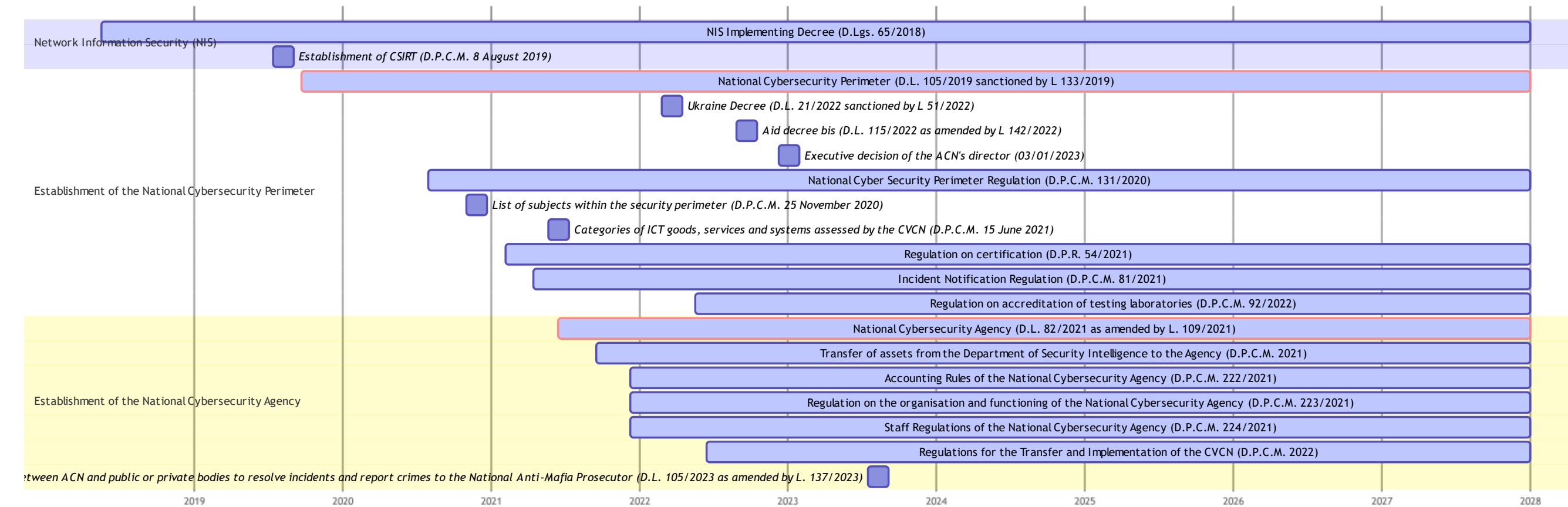




Figure 44 - Italian Cybersecurity Framework after the establishment of the National Perimeter

## V References

- '10th CSI/FBI Survey Shows Cybercrime Losses Down For Fourth Straight Year'. Accessed 17 June 2023. <https://www.crime-research.org/news/26.01.2006/1786/>.
- 87/95/EEC: Council Decision of 22 December 1986 on standardization in the field of information technology and telecommunications, 036 OJ L § (1986). <http://data.europa.eu/eli/dec/1987/95/oj/eng>.
- 'A Road Map for Digital Forensic Research'. Utica, New York: Digital Forensic Research Workshop, 7 August 2001. [https://dfrrs.org/wp-content/uploads/2019/06/2001\\_USA\\_a\\_road\\_map\\_for\\_digital\\_forensic\\_research.pdf](https://dfrrs.org/wp-content/uploads/2019/06/2001_USA_a_road_map_for_digital_forensic_research.pdf).
- Adele Anzon Demmig. 'Il Segreto Di Stato Ancora Una Volta Tra Presidente Del Consiglio, Autorità Giudiziaria e Corte Costituzionale'. *Giurisprudenza Costituzionale*, no. 2 (2009): 1020–33.
- . 'La Corte Abbandona Definitivamente All'esclusivo Dominio Dell'autorità Politica La Gestione Del Segreto Di Stato Nel Processo Penale'. *Giurisprudenza Costituzionale*, no. 1 (2012): 534–37.
- Adinolfi, Giovanna. 'States' Economic Measures to Counter Cyberattacks: Disentangling Their (Il)Legitimacy under International Law'. *Rivista Di Diritto Internazionale Privato e Processuale*, no. 3 (2022): 513–30.
- Adonis, Abid. 'International Law on Cyber Security in the Age of Digital Sovereignty'. *E-International Relations*, 2020. <https://www.e-ir.info/pdf/82169>.
- Agenzia per l'Italia digitale. 'CIRCOLARE 18 Aprile 2017, n. 2/2017 - Sostituzione Della Circolare n. 1/2017 Del 17 Marzo 2017, Recante: «Misure Minime Di Sicurezza ICT per Le Pubbliche Amministrazioni. (Direttiva Del Presidente Del Consiglio Dei Ministri 1° Agosto 2015)»', 18 April 2017. <https://www.gazzettaufficiale.it/eli/id/2017/05/05/17A03060/sg>.
- . 'Linee guida per lo sviluppo e la definizione del modello nazionale di riferimento per i CERT regionali', 13 February 2020. <https://docs.italia.it/AgID/documenti-inconsultazione/lg-cert-regionali/it/bozza/index.html>.
- . 'Strategia per la Crescita Digitale 2014-2020', 3 March 2015. [https://www.agid.gov.it/sites/default/files/repository\\_files/documentazione/strategia\\_crescita\\_digitale\\_ver\\_def\\_21062016.pdf](https://www.agid.gov.it/sites/default/files/repository_files/documentazione/strategia_crescita_digitale_ver_def_21062016.pdf).
- Agenzia per l'Italia Digitale and Dipartimento per la Trasformazione Digitale. 'Piano Triennale per l'informatica nella Pubblica Amministrazione 2020-2022', July 2020. [https://www.agid.gov.it/sites/default/files/repository\\_files/piano\\_triennale\\_per\\_l\\_informatica\\_nella\\_pa\\_2020\\_2022.pdf](https://www.agid.gov.it/sites/default/files/repository_files/piano_triennale_per_l_informatica_nella_pa_2020_2022.pdf).
- Alessandro Mantellero. 'Si rafforza la tutela dei dati personali: "data breach notification" e limiti alla profilazione mediante i "cookies"'. *Diritto dell'informazione e dell'informatica*, 2012.
- 'All News - European Commission'. Accessed 24 June 2023. <https://drmkc.jrc.ec.europa.eu/events-news/all-news#details21159>.
- Ammannati, Laura. 'Regolatori e Supervisorì Nell'era Digitale: Ripensare La Regolazione'. *Giurisprudenza Costituzionale*, no. 3 (2023): 1453–73.
- Anglmayer, Irmgard. 'European Critical Infrastructure - Revision of Directive 2008/114/EC'. Briefing. European Parliamentary Research Service, February 2021. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662604/EPRS\\_BRI\(2021\)0662604.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662604/EPRS_BRI(2021)0662604.pdf).

- 1)662604\_EN.pdf.
- Anzon, Adele. 'Interrogativi Sui Riflessi Sostanziali Della Nozione Di Segreto Di Stato Individuata Dalla Corte Costituzionale'. *Giurisprudenza Costituzionale*, no. 4–6 (1977): 866–69.
- 'Apertura Summer School Cybersicurezza'. Scuola Nazionale dell'Amministrazione, Roma, 12 July 2022. [https://www.funzionepubblica.gov.it/sites/funzionepubblica.gov.it/files/intervento\\_summerschool\\_cybersicurezza\\_0.pdf](https://www.funzionepubblica.gov.it/sites/funzionepubblica.gov.it/files/intervento_summerschool_cybersicurezza_0.pdf).
- Appazov, Artur. *Legal Aspects of Cybersecurity*. Copenhagen: Faculty of Law - University of Copenhagen, 2014. [https://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal\\_Aspects\\_of\\_Cybersecurity.pdf](https://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf).
- Arianna Vendaschi and Valerio Lubello. 'Data Retention and Its Implications for the Fundamental Right to Privacy: A European Perspective'. *Tilburg Law Review* 20, no. 1 (2015): 14–34. <https://doi.org/10.1163/22112596-02001005>.
- Armando, Alessandro, and Fabio Roli. 'Intelligenza Artificiale e "Cybersecurity". Fatti, Miti e Rischi'. *Gnosis*, no. 2 (2019): 143–51.
- Associazione Italiana per la Sicurezza Informatica. 'Rapporto Clusit 2018 sulla sicurezza ICT in Italia'. Clusit, September 2018. [https://clusit.it/wp-content/uploads/download/Rapporto\\_Clusit\\_2018\\_aggiornamento\\_settembre.pdf](https://clusit.it/wp-content/uploads/download/Rapporto_Clusit_2018_aggiornamento_settembre.pdf).
- . 'Rapporto Clusit 2019 sulla sicurezza ICT in Italia'. Clusit, September 2019. [https://clusit.it/wp-content/uploads/download/Rapporto\\_Clusit\\_2019\\_aggiornamento\\_settembre.pdf](https://clusit.it/wp-content/uploads/download/Rapporto_Clusit_2019_aggiornamento_settembre.pdf).
- . 'Rapporto Clusit 2020 sulla sicurezza ICT in Italia'. Clusit, March 2020. [https://clusit.it/wp-content/uploads/download/Rapporto\\_Clusit\\_2020\\_web\\_marzo.pdf](https://clusit.it/wp-content/uploads/download/Rapporto_Clusit_2020_web_marzo.pdf).
- Aterno, Stefano. *Sicurezza informatica: aspetti giuridici e tecnici*. Pacini giuridica 2. Pisa: Pacini, 2022.
- Ayalew, Yohannes Eneyew. 'The African Union's Malabo Convention on Cyber Security and Personal Data Protection Enters into Force Nearly after a Decade. What Does It Mean for Data Privacy in Africa or Beyond?' *EJIL:Talk! The Blog of the European Journal of International Law*, 1 January 2023. [https://www.academia.edu/103386834/The\\_African\\_Union\\_s\\_Malabo\\_Convention\\_on\\_Cyber\\_Security\\_and\\_Personal\\_Data\\_Protection\\_enters\\_into\\_force\\_nearly\\_after\\_a\\_decade\\_What\\_does\\_it\\_mean\\_for\\_Data\\_Privacy\\_in\\_Africa\\_or\\_beyond](https://www.academia.edu/103386834/The_African_Union_s_Malabo_Convention_on_Cyber_Security_and_Personal_Data_Protection_enters_into_force_nearly_after_a_decade_What_does_it_mean_for_Data_Privacy_in_Africa_or_beyond).
- Bagni, Filippo. 'The Regulatory Sandbox and the Cybersecurity Challenge: From the Artificial Intelligence Act to the Cyber Resilience Act'. *Rivista Italiana Di Informatica e Diritto*, no. 2 (2023): 201–17.
- Bak, Martin. 'European Electronic Communications on the Road to Full Competition: The Concept of Significant Market Power under the New Regulatory Framework'. *Journal of Network Industries* 4, no. 3 (2003): 293–324. <https://doi.org/10.1177/178359170300400303>.
- Bangemann group. 'Europe and the Global Information Society - Recommendations of the High-Level Group on the Information Society to the Corfu European Council (Bangemann Group)'. In *Growth, Competitiveness and Employment White Paper Follow-Up*. Luxembourg, 1994. [http://aei.pitt.edu/1199/1/info\\_society\\_bangeman\\_report.pdf](http://aei.pitt.edu/1199/1/info_society_bangeman_report.pdf).

- Bank, Inter American Development, and Organization of American States. 'Cybersecurity: Are We Ready in Latin America and the Caribbean?' *IDB Publications*, 14 March 2016. <https://doi.org/10.18235/0006517>.
- Banoth, Rajkumar, Narsimha Gugulothu, and Aruna Kranthi Godishala. *A Comprehensive Guide to Information Security Management and Audit*. First edition. Boca Raton: CRC Press, 2023.
- Barbara, Giovanni. 'La "Cybersecurity": Minacce, Evoluzione Normativa, "Corporate Governance" e Nuove Prospettive'. *Corporate Governance*, no. 4 (2022): 501–24.
- Barbareschi, Simone, and Andrea Giubilei. 'L'equilibrio tra la tutela dei dati personali e la manifestazione del pensiero'. In *I dati personali nel diritto europeo*, edited by Vincenzo Cuffaro, Roberto D'Orazio, and Vincenzo Ricciuto, 453–94. Torino: G. Giappichelli editore, 2019.
- Bassan, Fabio. *Diritto delle comunicazioni elettroniche: telecomunicazioni e televisione dopo la terza riforma comunitaria del 2009*. Milano: Giuffrè, 2010.
- Bavetta, Flavia. 'Direttiva NIS 2: Verso Un Innalzamento Dei Livelli Di Cybersicurezza a Livello Europeo - NIS'. *MediaLaws*, no. 3 (2022): 405–14.
- Beriaín, Iñigo de Miguel, Elena Atienza-Macías, and Emilio Armaza Armaza. 'The European Union Integrated Political Crisis Response Arrangements: Improving the European Union's Major Crisis Response Coordination Capacities'. *Disaster Medicine and Public Health Preparedness* 9, no. 3 (June 2015): 234–38. <https://doi.org/10.1017/dmp.2015.10>.
- Bianchi, Tazio. 'Firma Digitale e Ruolo Dell'Aipa Alla Luce Del d.Lgs. 23 Gennaio 2002, n. 10'. *Cyberspazio e Diritto*, no. 1 (2002): 1–7.
- Bieker, Felix, Michael Friedewald, Marit Hansen, Hannah Obersteller, and Martin Rost. 'A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation'. In *Privacy Technologies and Policy*, edited by Stefan Schiffner, Jetzabel Serna, Demosthenes Ikonou, and Kai Rannenberg, 9857:21–37. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2016. [https://doi.org/10.1007/978-3-319-44760-5\\_2](https://doi.org/10.1007/978-3-319-44760-5_2).
- Billois, G  r  me. 'Cybersecurity Incident and Crisis Management'. In *The Cyber Risk Handbook*, 171–84. John Wiley & Sons, Ltd, 2017. <https://doi.org/10.1002/9781119309741.ch12>.
- Body of European Regulators of Electronic Communications. 'BEREC Report on OTT Services', 29 January 2016. BoR (16) 35. [https://berec.europa.eu/eng/document\\_register/subject\\_matter/berec/reports/5751-berec-report-on-ott-services](https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services).
- Boin, Arjen, and Denis Smith. 'Terrorism and Critical Infrastructures: Implications for Public-Private Crisis Management'. *Public Money and Management* 26, no. 5 (November 2006): 295–304. <https://doi.org/10.1111/j.1467-9302.2006.00543.x>.
- Bonavita, Simone, Alessandro Cortina, and Elisabetta Stringhi. '"Conosci Il Tuo Nemico": Un Primo Approccio Tassonomico Ai Principali Attacchi Informatici Nel Settore "Cybercrime" Bancario e Finanziario'. *Cyberspazio e Diritto*, no. 3 (2020): 451–88.
- Bonetti, Paolo. 'Problemi Costituzionali Della Legge Di Riforma Dei Servizi Di Informazione per La Sicurezza Della Repubblica'. *Diritto e Societ  *, no. 2 (2008): 251–313.
- Brighi, Raffaella. 'Vulnerabilit   e Sicurezza: Un'analisi Informatico-Giuridica Di Concetti in Evoluzione'. *Notizie Di Politeia*, no. 136 (2019): 35–45.
- Brighi, Raffaella, and Pier Giorgio Chiara. 'La Cybersecurity Come Bene Pubblico: Alcune Riflessioni Normative a Partire Dai Recenti Sviluppi Nel Diritto UE'. *Federalismi.It*, no.

- 21 (8 September 2021): 18–42.
- Brignoli, Mauro Alberto. 'Analisi e Studio Di Una Soluzione Innovativa a Complemento Del GDPR per Promuovere La Cultura Della Sicurezza Informatica in Europa'. *Cyberspazio e Diritto*, no. 1–2 (2018): 225–44.
- Brown, Neil. 'An Assessment of the Proportionality of Regulation of "over the Top" Communications Services under Europe's Common Regulatory Framework for Electronic Communications Networks and Services'. *Computer Law & Security Review* 30, no. 4 (2014): 357–74. <https://doi.org/10.1016/j.clsr.2014.05.010>.
- Buffa, Matteo. 'La Direttiva NIS II Cybersecurity in Europa: Tra Innovazione, Formazione e Diritto Vivente'. *Democrazia e Diritti Sociali*, no. 1 (2023): 47–64.
- Burgess, J. Peter. 'Social Values and Material Threat: The European Programme for Critical Infrastructure Protection'. *International Journal of Critical Infrastructures* 3, no. 3–4 (January 2007): 471–87. <https://doi.org/10.1504/IJCIS.2007.014121>.
- Buttarelli, Gianluca. 'La Regolazione Delle Piattaforme Digitali: Il Ruolo Delle Istituzioni Pubbliche'. *Giornale Di Diritto Amministrativo*, no. 1 (2023): 116–27.
- Califano, Licia. 'Chat GPT e Meta ["Meta Platforms Ireland Limited" - MPIL] EDI ["Election Day Information"]': Spunti Problematici Su Profili Regolatori e Ruolo Delle Autorità Di Controllo Di Protezione Dati'. *Federalismi.It*, no. 10 (2023): 4–15.
- 'Canadian Trusted Computer Product Evaluation Criteria'. In *Wikipedia*. Accessed 2 November 2022. [https://en.wikipedia.org/w/index.php?title=Canadian\\_Trusted\\_Computer\\_Product\\_Evaluation\\_Criteria&oldid=1103502712](https://en.wikipedia.org/w/index.php?title=Canadian_Trusted_Computer_Product_Evaluation_Criteria&oldid=1103502712).
- Caputo, Barbara. 'La Visione Computerizzata Dell'era Del "Deep Learning". Sfide e Opportunità per La "Cybersecurity"'. *Gnosis*, no. 2 (2017): 90–95.
- Carchidi, Fabio. 'Perimetro Di Sicurezza Nazionale Cibernetica, Dal d.l. 105/2019 Ai d.p.c.m. n. 131/2020 e n. 81/2021: La Sublimazione Delle Cc.Dd. "Information and Communication Technologies"'. *Ambienteditto.it*, no. 3 (2021): 295–305.
- Carotti, Bruno. 'Il Correttivo al Codice Dell'amministrazione Digitale: Una Meta-Riforma'. *Giornale Di Diritto Amministrativo*, no. 2 (2018): 131–41.
- . 'Sicurezza Cibernetica e Stato-Nazione'. *Giornale Di Diritto Amministrativo*, no. 5 (2020): 629–41.
- Carpentieri, Renata. 'L'Agenda Digitale Italiana'. *Giornale Di Diritto Amministrativo*, no. 3 (2013): 225–33.
- Carrapiço, Helena, and Florian Trauner. 'Europol and Its Influence on EU Policy-Making on Organized Crime: Analyzing Governance Dynamics and Opportunities'. *Perspectives on European Politics and Society* 14, no. 3 (September 2013): 357–71. <https://doi.org/10.1080/15705854.2013.817804>.
- Carrier, Brian D., and E. Spafford. 'Getting Physical with the Digital Investigation Process'. *International Journal of Digital Evidence* 2, no. 2 (2003).
- Casarosa, Federica. 'L'armonizzazione Degli Obblighi Di Notifica: Il DDL Cybersicurezza Fra La NIS 2'. *Rivista Italiana Di Informatica e Diritto*, no. 1 (2024): 11–14.
- Case of S. and Marper v. The United Kingdom, No. 30562/04 e 30566/04 (European Court of Human Rights 4 December 2008).
- Casino, Fran, Tom Dasaklis, Georgios Spathoulas, Marios Anagnostopoulos, Amrita Ghosal, Istvan Borocz, Agusti Solanas, Mauro Conti, and Constantinos Patsakis. 'Research Trends, Challenges, and Emerging Topics of Digital Forensics: A Review of Reviews'. arXiv, 10 January 2022. <https://doi.org/10.48550/arXiv.2108.04634>.

- Castelli, Luca. *L'autodichia Degli Organi Costituzionali: Assetti, Revisioni, Evoluzioni*. Per Una Koiné Costituzionale 12. Torino: G. Giappichelli Editore, 2019.
- Casu, Antonio. 'Parlamento e Sicurezza Nazionale.' *Bollettino Di Informazioni Costituzionali e Parlamentari*, no. 2 (1994): 227–49.
- Cavanna, Valentina. 'Nuovi Poteri, Vecchi Problemi. Il Costituzionalismo Alla Prova Del Digitale'. *Diritto Pubblico Comparato Ed Europeo*, no. 1 (2023): 223–48.
- Centre for Europe, University of Warsaw, Poland, and Marta Grabowska. 'Legal, Political and Organizational Aspects of Cybersecurity in the European Union'. *On-Line Journal Modelling the New Europe*, no. 38 (9 April 2022): 106–32. <https://doi.org/10.24193/OJMNE.2022.38.05>.
- CEPR. 'The Failure of the Lisbon Strategy', 12 January 2010. <https://cepr.org/voxeu/columns/failure-lisbon-strategy>.
- Chayes, Abram, and Antonia Handler Chayes. *The New Sovereignty*. Harvard University Press, 1995. <https://doi.org/10.4159/9780674029453>.
- Chiara, Pier Giorgio. 'Il "Cyber Resilience Act": La Proposta Di Regolamento Della Commissione Europea Relativa a Misure Orizzontali Di Cybersicurezza per Prodotti Con Elementi Digitali'. *Rivista Italiana Di Informatica e Diritto*, no. 1 (2023): 143–53.
- Christiansen, Thomas, and Christine Neuhold. 'Informal Politics in the EU: Informal Politics in the EU'. *JCMS: Journal of Common Market Studies* 51, no. 6 (November 2013): 1196–1206. <https://doi.org/10.1111/jcms.12068>.
- Christou, George. 'The Collective Securitisation of Cyberspace in the European Union'. *West European Politics* 42, no. 2 (23 February 2019): 278–301. <https://doi.org/10.1080/01402382.2018.1510195>.
- . 'The European Union and Cybercrime'. In *Cybersecurity in the European Union*, 87–118. London: Palgrave Macmillan UK, 2016. [https://doi.org/10.1057/9781137400529\\_5](https://doi.org/10.1057/9781137400529_5).
- Ciaurro, Gian Franco. 'Prerogative Costituzionali'. In *Enciclopedia Del Diritto*. Giuffré Francis Lefebvre, 1986.
- Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. 1st ed. New York: HarperCollins, 2010.
- Clarke, Roger. 'Privacy Impact Assessment: Its Origins and Development'. *Computer Law & Security Review* 25, no. 2 (January 2009): 123–35. <https://doi.org/10.1016/j.clsr.2009.02.002>.
- Cocchi, Tommaso. 'La Cybersicurezza Nel Prisma Del Diritto Dei Contratti Pubblici: Un Tentativo Di Ricostruzione Delle Regole Del Gioco Tra Requisiti Di Partecipazione, Criteri Di Aggiudicazione Ed Esigenze Di Certezza'. *Munus*, no. 1 (2024): 177–207.
- Cocco, G. 'Modi e Forme Di Esercizio Dell'attività Informativa e Di Sicurezza Nel Regime Precedente La L. 24 Ottobre 1977, N. 801'. In *I Servizi Di Informazione e Di Sicurezza Nell'ordinamento Italiano*, 95–154. Padova, Italy, 1980.
- . 'Vicende Storiche e Deviazioni Dei Servizi Di Informazione e Di Sicurezza'. In *I Servizi Di Informazione e Di Sicurezza Nell'ordinamento Italiano*, 173–229. Padova, Italy, 1980.
- Colapietro, Carlo. *Il diritto alla protezione dei dati personali in un sistema delle fonti multilivello: il Regolamento UE 2016/679 parametro di legittimità della complessiva normativa italiana sulla 'privacy'*. Napoli: Editoriale scientifica, 2018.
- . 'Libera Manifestazione Del Pensiero, Fake News e Privacy, Oggi'. *Dirittifondamentali.It*, no. 2 (2022): 422–38.

- Cole, Mark, and Sandra Schmitz. 'The Interplay Between the NIS Directive and the GDPR in a Cybersecurity Threat Landscape'. *SSRN Electronic Journal*, 2019. <https://doi.org/10.2139/ssrn.3512093>.
- Comandè, Giovanni, and Federica Casarosa. 'Aspettando La NIS2 ["Network and Information Systems"]': Ovvero Il Diritto Privato Della "Cybersecurity". *Il Diritto Dell'informazione e Dell'informatica*, no. 1 (2024): 29–53.
- Comitato di Presidenza del Consiglio Superiore della Magistratura. 'ORDINE DEL GIORNO AGGIUNTO - 1265/AC/2023', 6 March 2024. <https://www.csm.it/web/csm-internet/lavori-del-consiglio/dal-plenum?datalink=1709719200000&titololink=seduta+plenum+ordinaria&idAppuntamento=11581#>.
- Comitato Parlamentare per la Sicurezza della Repubblica. 'RELAZIONE sulle politiche e gli strumenti per la protezione cibernetica e la sicurezza informatica, a tutela dei cittadini, delle istituzioni, delle infrastrutture critiche e delle imprese di interesse strategico nazionale'. XXXIV. Comitato Parlamentare per la Sicurezza della Repubblica, dicembre 2019. [https://documenti.camera.it/\\_dati/leg18/lavori/documentiparlamentari/IndiceETesti/034/001/intero.pdf](https://documenti.camera.it/_dati/leg18/lavori/documentiparlamentari/IndiceETesti/034/001/intero.pdf).
- . 'RELAZIONE sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico'. XXXIV. Comitato Parlamentare per la Sicurezza della Repubblica, 7 July 2010. [https://www.parlamento.it/documenti/repository/commissioni/bicamerali/COMITATO%20SICUREZZA/Doc\\_XXXIV\\_n\\_4.pdf](https://www.parlamento.it/documenti/repository/commissioni/bicamerali/COMITATO%20SICUREZZA/Doc_XXXIV_n_4.pdf).
- 'Common Criteria: New CC Portal'. Accessed 30 April 2023. <https://www.commoncriteriaportal.org/>.
- 'Computer Security Institute'. In *Wikipedia*, 24 March 2023. [https://en.wikipedia.org/w/index.php?title=Computer\\_Security\\_Institute&oldid=1146421118](https://en.wikipedia.org/w/index.php?title=Computer_Security_Institute&oldid=1146421118).
- Consiglio di Stato. 'Schema di decreto del Presidente del Consiglio dei ministri (d.P.C.M.) in materia di perimetro di sicurezza nazionale cibernetica, adottato in attuazione dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133', 21 May 2020. [https://www.giustizia-amministrativa.it/portale/pages/istituzionale/visualizza/?nodeRef=&schema=consul&nrg=202000417&nomeFile=202000983\\_27.html&subDir=Provvedimenti](https://www.giustizia-amministrativa.it/portale/pages/istituzionale/visualizza/?nodeRef=&schema=consul&nrg=202000417&nomeFile=202000983_27.html&subDir=Provvedimenti).
- Contaldo, Alfonso. 'L'attuazione Della "Cybersecurity" Nazionale: Un Difficile Esercizio Di Una Funzione Pubblica'. *Lo Stato*, no. 21 (2023): 283–97.
- . 'L'ENISA e Le Competenze Comunitarie per La Cibersicurezza'. *Rivista Di Polizia*, no. 6–7 (2018): 655–81.
- Contaldo, Alfonso, and Davide Mula. *Cybersecurity law: disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche*. Pisa: Pacini giuridica, 2020.
- Contaldo, Alfonso, and Flaviano Peluso. 'La Protezione Delle Infrastrutture Critiche Nell'ordinamento Giuridico Italiano e Dell'Unione Europea'. *Rivista Amministrativa Della Repubblica Italiana*, no. 5–6 (2015): 225–48.
- Costanzo, Pasquale. 'Lo "stato digitale": considerazioni introduttive', 11–36. Genova, 2021.
- Council of Europe. 'Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data', 28 January 1981. <https://rm.coe.int/1680078b37>.

- Council of the European Communities. 87/499/EEC: Council Decision of 5 October 1987 introducing a communications network Community programme on trade electronic data interchange systems (TEDIS), Pub. L. No. 499, EEC (1987). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31987D0499>.
- . ‘98/560/EC: Council Recommendation of 24 September 1998 on the Development of the Competitiveness of the European Audiovisual and Information Services Industry by Promoting National Frameworks Aimed at Achieving a Comparable and Effective Level of Protection of Minors and Human Dignity’. *OJ L*, 24 September 1998. <http://data.europa.eu/eli/reco/1998/560/oj/eng>.
  - . Commission Directive 88/301/EEC of 16 May 1988 on competition in the markets in telecommunications terminal equipment, Pub. L. No. 301, EEC (1988). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31988L0301>.
  - . Council Directive 86/361/EEC of 24 July 1986 on the initial stage of the mutual recognition of type approval for telecommunications terminal equipment, Pub. L. No. 361, EEC (1986). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31986L0361>.
  - . Council Directive 90/387/EEC of 28 June 1990 on the establishment of the internal market for telecommunications services through the implementation of open network provision, Pub. L. No. 387, EEC (1990). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31990L0387>.
  - . Council Directive 91/263/EEC of 29 April 1991 on the approximation of the laws of the Member States concerning telecommunications terminal equipment, including the mutual recognition of their conformity, Pub. L. No. 263, EEC (1991). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31991L0263>.
- Council of the European Union. 2014/415/EU: Council Decision of 24 June 2014 on the arrangements for the implementation by the Union of the solidarity clause, 192 *OJ L* § (2014). <http://data.europa.eu/eli/dec/2014/415/oj/eng>.
- . ‘A Strategic Compass for Security and Defence - For a European Union That Protects Its Citizens, Values and Interests and Contributes to International Peace and Security’, 21 March 2022. 7371/22. <https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf>.
  - . ‘Common Position (EC) No 39/2003 of 26 May 2003 Adopted by the Council, Acting in Accordance with the Procedure Referred to in Article 251 of the Treaty Establishing the European Community, with a View to Adopting a Decision of the European Parliament and of the Council Adopting a Multiannual Programme (2003 to 2005) for the Monitoring of the eEurope 2005 Action Plan, Dissemination of Good Practices and the Improvement of Network and Information Security (MODINIS)’, 26 May 2003. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52003AG0039>.
  - . ‘Common Security and Defence Policy’, 19 December 2013. [https://www.consilium.europa.eu/uedocs/cms\\_data/docs/pressdata/en/ec/140214.pdf](https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/140214.pdf).
  - . ‘Complementary Efforts to Enhance Resilience and Counter Hybrid Threats - Council Conclusions (10 December 2019)’, 10 December 2019. <https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/en/pdf>.
  - . ‘Conclusions of the Council of the European Union on Critical Information Infrastructure Protection “Achievements and next Steps: Towards Global Cyber-Security”’, 19 May 2011. <https://data.consilium.europa.eu/doc/document/ST-10299->



- 2011-INIT/en/pdf.
- . ‘Council Conclusions on Shaping Europe’s Digital Future’, 16 June 2020. 2020/C 202 I/01. [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020XG0616\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020XG0616(01)).
  - . ‘Council Conclusions on Strengthening Resilience and Countering Hybrid Threats, Including Disinformation in the Context of the COVID-19 Pandemic’, 15 December 2020. 13626/20. <https://data.consilium.europa.eu/doc/document/ST-14064-2020-INIT/en/pdf>.
  - . ‘Council Conclusions on the Cybersecurity of Connected Devices - Council Conclusions Approved by Written Procedure’, 2 December 2020. <https://data.consilium.europa.eu/doc/document/ST-13629-2020-INIT/en/pdf>.
  - . ‘Council Conclusions on the EU Policy on Cyber Defence’, 22 May 2023. <https://www.consilium.europa.eu/media/64526/st09618-en23.pdf>.
  - . Council Decision (CFSP) 2017/2315 of 11 December 2017 establishing permanent structured cooperation (PESCO) and determining the list of participating Member States, 331 OJ L § (2017). <http://data.europa.eu/eli/dec/2017/2315/oj/eng>.
  - . Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, 129I OJ L § (2019). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019D0797>.
  - . Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, 246 OJ L § (2020). <http://data.europa.eu/eli/dec/2020/1127/oj/eng>.
  - . Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Pub. L. No. 345, OJ L (2008). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114>.
  - . Council framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography, 013 OJ L § (2003). [http://data.europa.eu/eli/dec\\_framw/2004/68/oj/eng](http://data.europa.eu/eli/dec_framw/2004/68/oj/eng).
  - . Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems (2005). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32005F0222&qid=1659969013825>.
  - . Council Implementing Decision (EU) 2018/1993 of 11 December 2018 on the EU Integrated Political Crisis Response Arrangements, 320 OJ L § (2018). [http://data.europa.eu/eli/dec\\_impl/2018/1993/oj/eng](http://data.europa.eu/eli/dec_impl/2018/1993/oj/eng).
  - . Council Implementing Regulation (EU) 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, 246 OJ L § (2020). [http://data.europa.eu/eli/reg\\_impl/2020/1125/oj/eng](http://data.europa.eu/eli/reg_impl/2020/1125/oj/eng).
  - . ‘Council Recommendation of 7 April 1995 on Common Information Technology Security Evaluation Criteria’, 7 April 1995. 95/144/EC. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995H0144>.
  - . ‘Council Recommendation of 8 December 2022 on a Union-Wide Coordinated Approach to Strengthen the Resilience of Critical Infrastructure (Text with EEA Relevance) 2023/C 20/01’, 20 January 2023. 2023/C 20/01. <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32023H0120%2801%29>.
  - . ‘Council Recommendation of 25 June 2001 on Contact Points Maintaining a 24-Hour

- Service for Combating High-Tech Crime’, 25 June 2001. OJ C 187, 3.7.2001, p. 5–6. [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32001H0703\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32001H0703(01)).
- . Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, 129I OJ L § (2019). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0796>.
- . ‘Council Resolution of 28 January 2002 on a Common Approach and Specific Actions in the Area of Network and Information Security’, 28 January 2002. OJ C 43, 16.2.2002, p. 2–4. [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002G0216\(02\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002G0216(02)).
- . ‘Declaration on Combating Terrorism’, 25 March 2004. [https://www.consilium.europa.eu/uedocs/cms\\_data/docs/pressdata/en/ec/79637.pdf](https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/79637.pdf).
- . ‘Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (“Cyber Diplomacy Toolbox”)', 7 June 2017. 9916/17. <https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf>.
- . ‘EU Cyber Defence Policy Framework’, 18 November 2014. <https://ccdcoe.org/uploads/2018/11/EU-141118-EUCyberDefencePolicyFrame-2.pdf>.
- . ‘European Council 19/20 December 2013 Conclusions’, 20 December 2013. EUCO 217/13. [https://www.consilium.europa.eu/uedocs/cms\\_data/docs/pressdata/en/ec/140245.pdf](https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/140245.pdf).
- . ‘In the Field of Security of Information Systems’, 31 March 1992. 92/242/EEC. <https://op.europa.eu/en/publication-detail/-/publication/2b0db115-a244-464f-a4ab-2e28d1a5a9ab>.
- . ‘Lisbon European Council 23-24.03.2000: Conclusions of the Presidency’, 23 March 2000. [https://www.europarl.europa.eu/summits/lis1\\_en.htm?textMode=on](https://www.europarl.europa.eu/summits/lis1_en.htm?textMode=on).
- . ‘Presidency Conclusions – Brussels, 17 and 18 June 2004’, 17 June 2004. <https://data.consilium.europa.eu/doc/document/ST-10679-2004-REV-2/en/pdf>.
- . ‘Presidency Conclusions - European Council Stockholm’, 26 March 2001. [http://aei.pitt.edu/43341/1/Stockholm\\_2001.pdf](http://aei.pitt.edu/43341/1/Stockholm_2001.pdf).
- . ‘Rapid Alert System - Strengthening Coordinated and Joint Responses to Disinformation’, March 2019. [https://www.eeas.europa.eu/sites/default/files/documents/ras\\_factsheet\\_march\\_2019\\_0.pdf](https://www.eeas.europa.eu/sites/default/files/documents/ras_factsheet_march_2019_0.pdf).
- . ‘Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union’s Foreign and Security Policy’, June 2016. [https://www.eeas.europa.eu/sites/default/files/eugs\\_review\\_web\\_0.pdf](https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf).
- . ‘Special Meeting of the European Council (1 and 2 October 2020) – Conclusions’, 2 October 2020. <https://data.consilium.europa.eu/doc/document/ST-13-2020-INIT/en/pdf>.
- . ‘The Hague Programme: Strengthening Freedom, Security and Justice in the European Union’, 3 March 2005. 2005/C 53/01. [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52005XG0303\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52005XG0303(01)).
- . ‘The Stockholm Programme — An Open and Secure Europe Serving and Protecting Citizens’, 4 May 2010. 2010/C 115/01. <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:EN:PDF>.

- Council of the European Union and European Parliament. 'Decision No 2256/2003/EC of the European Parliament and of the Council of 17 November 2003 Adopting a Multiannual Programme (2003-2005) for the Monitoring of the eEurope 2005 Action Plan, Dissemination of Good Practices and the Improvement of Network and Information Security (MODINIS)', 17 November 2003. OJ L 336, 23.12.2003, p. 1–5. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003D2256>.
- . Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (2013). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013L0040>.
- . Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, 077 OJ L § (2004). <http://data.europa.eu/eli/reg/2004/460/oj/eng>.
- . Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, 202 OJ L § (2021). <http://data.europa.eu/eli/reg/2021/887/oj/eng>.
- Council of the European Union and NATO. 'Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization', 8 July 2016. <https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf>.
- Council Resolution of 30 June 1988 on the development of the common market for telecommunications services and equipment up to 1992 (1988). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31988Y1004%2801%29>.
- 'Critical Infrastructure Warning Information Network (CIWIN)'. Accessed 24 June 2023. [https://home-affairs.ec.europa.eu/networks/critical-infrastructure-warning-information-network-ciwin\\_en](https://home-affairs.ec.europa.eu/networks/critical-infrastructure-warning-information-network-ciwin_en).
- Czech Republic v European Parliament and Council of the European Union, No. Case C-482/17 (ECJ 3 December 2019).
- D'Acquisto, Giuseppe, and Maurizio Naldi. *Big data e privacy by design: anonimizzazione, pseudonimizzazione, sicurezza*. I diritti nella rete della rete 5. Torino: G. Giappichelli, 2017.
- Dalle Nogare, Fabrizio. 'Le comunicazioni elettroniche: evoluzione del quadro istituzionale e prospettive'. In *Regolazione e mercato delle comunicazioni elettroniche: la storia, la governance delle regole e il nuovo Codice europeo*, 1–76. Torino: G. Giappichelli Editore, 2019.
- David H. Flaherty. 'Privacy Impact Assessments: An Essential Tool for Data Protection'. In *New Technologies, Security and Freedom*. Venice, 2000. <https://aspe.hhs.gov/privacy-impact-assessment-essential-tool-data-protection>.
- Davidoff, Sherri, and Jonathan Ham. *Network Forensics: Tracking Hackers through Cyberspace*. Upper Saddle River, NJ: Prentice Hall, 2012.
- De Liutiis, G. *Storia Dei Servizi Segreti in Italia*. Roma, Italy, 1985.
- De Minico, Giovanna. 'La risposta europea al terrorismo del tempo ordinario: il "lawmaker" e il giudice'. *Osservatorio sulle fonti*, no. 2 (2017): 19.
- Decision No 1673/2006/EC of the European Parliament and of the Council of 24 October 2006 on the financing of European standardisation, 315 OJ L § (2006).

- <http://data.europa.eu/eli/dec/2006/1673/oj/eng>.
- ‘DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 17 febbraio 2017’, 02 2017. <https://www.gazzettaufficiale.it/eli/id/2017/04/13/17A02655/sg>.
- ‘DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 24 gennaio 2013’, 24 January 2013. <https://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg>.
- Delle Donne, Clarice. ‘Autodichia Degli Organi Costituzionali e Universalità Della Giurisdizione Nella Cornice Dello Stato Di Diritto: La Corte Costituzionale Fa Il Punto’. *Rivista Trimestrale Di Diritto e Procedura Civile*, no. 1 (2015): 141–64.
- . ‘La Questione Di Autodichia Nel Processo (Ovvero Degli Incerti Confini Tra Regolamento Di Giurisdizione e Conflitto Di Attribuzioni)’. *Judicium*, no. 3 (2020): 301–24.
- Demetzou, Katerina. ‘Data Protection Impact Assessment: A Tool for Accountability and the Unclarified Concept of “High Risk” in the General Data Protection Regulation’. *Computer Law & Security Review* 35, no. 6 (November 2019): 105342. <https://doi.org/10.1016/j.clsr.2019.105342>.
- Deming, W. Edwards. *Out of the Crisis*. The MIT Press, 2018. <https://doi.org/10.7551/mitpress/11457.001.0001>.
- DeNardis, Laura. *The Global War for Internet Governance*. Yale University Press, 2014. <https://doi.org/10.12987/yale/9780300181357.001.0001>.
- Dewar, Robert S. ‘Cyber-Lisbon? The Impact of the Treaty of Lisbon on European Union Cybersecurity Policy’, 2015. <https://eustudies.org/conference/papers/download/107>.
- Di Palma, Pierluigi, and Francesco Gaspari. ‘L’attuazione Del “Golden Power” in Italia: Dal Potere Regolamentare Alla Potestà Regolatoria’. *GiustAmm.It*, no. 4 (2013): 40.
- Dipartimento Informazioni per la Sicurezza. ‘Relazione sulla politica dell’informazione per la sicurezza’. Dipartimento Informazioni per la Sicurezza, 2009. <https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2010/02/relazione-2009.pdf>.
- Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations, 204 OJ L § (1998). <http://data.europa.eu/eli/dir/1998/34/oj/eng>.
- Düll, Andreas, Anja Schoch, and Matthias Straub. ‘Cybersecurity in the European Union’. *Central and Eastern European eDem and eGov Days* 331 (12 July 2018): 313–23. <https://doi.org/10.24989/ocg.v331.26>.
- Dusanovic, Darja. ‘Implications of Invalidity of Data Retention Directive to Telecom Operators’. *Juridical Tribune Journal = Tribuna Juridica* 4, no. 2 (2014): 44–60.
- ENISA. ‘EU CyCLONe’. Topic. Accessed 31 August 2023. <https://www.enisa.europa.eu/topics/incident-response/cyclone>.
- ENISA. ‘Good Practices for Supply Chain Cybersecurity’, June 2023. <https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity/@download/fullReport>.
- . ‘National/Governmental CERTs ENISA’s Recommendations on Baseline Capabilities’, December 2014. <https://www.enisa.europa.eu/publications/national-governmental-certs-enisas-recommendations-on-baseline-capabilities/@download/fullReport>.
- ENISA. ‘Threat Taxonomy’. File. Accessed 13 November 2023. <https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view>.
- ‘Enisa Threat Landscape 2022’. Threat Landscape. European Union Agency for Cybersecurity,

- November 2022. <https://data.europa.eu/doi/10.2824/324797>.
- European Commission. 'Amended Proposal for a Council Recommendation on Common Information Technology Security Evaluation Criteria', 9 February 1994. COM/94/37FINAL. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:51994PC0037>.
- . 'An EU Cybercrime Centre to Fight Online Criminals and Protect E-Consumers', 28 March 2012. [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_12\\_317](https://ec.europa.eu/commission/presscorner/detail/en/IP_12_317).
- . Commission Directive 90/388/EEC of 28 June 1990 on competition in the markets for telecommunications services, Pub. L. No. 388, EEC (1990). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31990L0388>.
- . Commission Directive 94/46/EC of 13 October 1994 amending Directive 88/301/EEC and Directive 90/388/EEC in particular with regard to satellite communications, 268 OJ L § (1994). <http://data.europa.eu/eli/dir/1994/46/oj/eng>.
- . Commission Directive 95/51/EC of 18 October 1995 amending Directive 90/388/EEC with regard to the abolition of the restrictions on the use of cable television networks for the provision of already liberalized telecommunications services, 256 OJ L § (1995). <http://data.europa.eu/eli/dir/1995/51/oj/eng>.
- . Commission Directive 96/2/EC of 16 January 1996 amending Directive 90/388/EEC with regard to mobile and personal communications, 020 OJ L § (1996). <http://data.europa.eu/eli/dir/1996/2/oj/eng>.
- . Commission Directive 96/19/EC of 13 March 1996 amending Directive 90/388/EEC with regard to the implementation of full competition in telecommunications markets, 074 OJ L § (1996). <http://data.europa.eu/eli/dir/1996/19/oj/eng>.
- . 'Commission Implementing Decision (EU) 2017/179 of 1 February 2017 Laying down Procedural Arrangements Necessary for the Functioning of the Cooperation Group Pursuant to Article 11(5) of the Directive (EU) 2016/1148 of the European Parliament and of the Council Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union', 2 February 2017. C/2017/0438. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017D0179>.
- . 'Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 Laying down Rules for Application of Directive (EU) 2016/1148 of the European Parliament and of the Council as Regards Further Specification of the Elements to Be Taken into Account by Digital Service Providers for Managing the Risks Posed to the Security of Network and Information Systems and of the Parameters for Determining Whether an Incident Has a Substantial Impact', 30 January 2018. C/2018/0471. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R0151>.
- . 'Commission Recommendation (EU) 2017/1584 of 13 September 2017 on Coordinated Response to Large-Scale Cybersecurity Incidents and Crises'. OJ L, 13 September 2017. <http://data.europa.eu/eli/reco/2017/1584/oj/eng>.
- . 'Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G Networks', 26 March 2019. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019H0534>.
- . 'COMMISSION RECOMMENDATION on Building a Joint Cyber Unit', 23 June 2021. C(2021) 4520 final. <https://ec.europa.eu/newsroom/dae/redirection/document/77514>.
- . 'COMMISSION STAFF WORKING DOCUMENT - Union Rolling Work Programme for European Cybersecurity Certification', 7 February 2024.

- <https://ec.europa.eu/newsroom/dae/redirection/document/102292>.
- . ‘Commission Staff Working Document - Assessment of the EU 2013 Cybersecurity Strategy’, 13 September 2017. SWD(2017) 295 final. [https://ec.europa.eu/transparency/documents-register/api/files/SWD\(2017\)295\\_0/de00000000176037?rendition=false](https://ec.europa.eu/transparency/documents-register/api/files/SWD(2017)295_0/de00000000176037?rendition=false).
  - . ‘COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the Document Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Ensure a High Level of Network and Information Security across the Union’, 7 February 2013. SWD(2013) 32 final.
  - . ‘COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Accompanying the Document Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity across the Union, Repealing Directive (EU) 2016/1148’, 16 December 2020. SWD(2020) 345 final. [https://eur-lex.europa.eu/resource.html?uri=cellar:d51e4bbb-3fa8-11eb-b27b-01aa75ed71a1.0001.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:d51e4bbb-3fa8-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF).
  - . ‘COMMISSION STAFF WORKING DOCUMENT on a New Approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures More Secure’, 28 August 2013. [https://home-affairs.ec.europa.eu/system/files/2020-09/swd\\_2013\\_318\\_on\\_epcip\\_en.pdf](https://home-affairs.ec.europa.eu/system/files/2020-09/swd_2013_318_on_epcip_en.pdf).
  - . ‘Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCIP)’, 22 June 2012. SWD(2012) 190 final. [https://home-affairs.ec.europa.eu/system/files/2020-09/epcip\\_swd\\_2012\\_190\\_final.pdf](https://home-affairs.ec.europa.eu/system/files/2020-09/epcip_swd_2012_190_final.pdf).
  - . ‘Communication from the Commission on a European Programme for Critical Infrastructure Protection’, 12 December 2006. COM(2006) 786 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52006DC0786&qid=1687081895752>.
  - . ‘Communication from the Commission to the Council and European Parliament - The eEurope 2002 Update Prepared by the European Commission for the European Council in Nice, 7th and 8th December 2000’, 29 November 2000. COM/2000/0783 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52000DC0783&qid=1685684370134>.
  - . ‘Communication from the Commission to the Council and the European Parliament - Critical Infrastructure Protection in the Fight against Terrorism’, 20 October 2004. COM/2004/0702 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52004DC0702&qid=1685943519045>.
  - . ‘Communication from the Commission to the Council and the European Parliament - eEurope 2002: Impact and Priorities A Communication to the Spring European Council in Stockholm, 23-24 March 2001’, 13 March 2001. COM/2001/0140 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52001DC0140>.
  - . ‘Communication from the Commission to the Council and the European Parliament - Preparedness and Consequence Management in the Fight against Terrorism’, 20 October 2004. COM(2004) 701 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52004DC0701&qid=1687082120625>.
  - . ‘Communication from the Commission to the Council and the European Parliament - Prevention, Preparedness and Response to Terrorist Attacks’, 20 October 2004. COM/2004/0698 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52004DC0698&qid=1687082120625>.

- content/EN/TXT/?uri=CELEX:52004DC0698.
- . ‘Communication from the Commission to the Council and the European Parliament and to the Economic and Social Committee and the Committee of Regions - Europe’s Way to the Information Society. An Action Plan’, 19 July 1994. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A51994DC0347&qid=1682951576431>.
  - . ‘COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT Tackling Crime in Our Digital Age: Establishing a European Cybercrime Centre’, 28 March 2012. COM/2012/0140 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52012DC0140&qid=1688740740533>.
  - . ‘Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - eEurope 2002 Final Report’, 11 February 2003. COM/2003/0066 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52003DC0066&qid=1685639413472>.
  - . ‘Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - eEurope 2005: An Information Society for All - An Action Plan to Be Presented in View of the Sevilla European Council, 21/22 June 2002’, 28 May 2002. COM/2002/0263 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52002DC0263>.
  - . ‘Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - eEurope Benchmarking Report - eEurope 2002’, 5 February 2002. COM/2002/0062 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52002DC0062&qid=1685639413472>.
  - . ‘Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - Globalisation and the Information Society - The Need for Strengthened International Coordination’, 4 February 1998. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A51998DC0050&qid=1683984191563>.
  - . ‘Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - Illegal and Harmful Content on the Internet’, 16 October 1996. COM/96/0487 FINAL. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A51996DC0487&qid=1684518587373>.
  - . ‘Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - Towards a New Framework for Electronic Communications Infrastructure and Associated Services - The 1999 Communications Review’, 10 November 1999. COM/99/0539 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:51999DC0539>.
  - . ‘COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime’, 26 January 2001. <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52000DC0890>.
  - . ‘Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - A

- Strategy for a Secure Information Society - “Dialogue, Partnership and Empowerment”, 31 May 2006. COM(2006) 251 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52006DC0251&qid=1683984996443>.
- . ‘Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - eEurope 2005 Action Plan: An Update {SEC(2004) 607} {SEC(2004) 608}’, 17 May 2004. COM/2004/0380 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52004DC0380&qid=1685698009806>.
- . ‘Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - eEurope 2005 Mid-Term Review’, 18 February 2004. COM/2004/0108 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52004DC0108&qid=1685698009806>.
- . ‘Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - “I2010 – A European Information Society for Growth and Employment”, 1 June 2005. COM(2005) 229 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52005DC0229>.
- . ‘Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach’, 6 June 2001. COM/2001/0298 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52001DC0298>.
- . ‘Communication from the Commission to the European Parliament and the Council - Draft Action Plan for the Single Market’, 6 May 1997. COM/97/0184 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A51997DC0184&qid=1684500102416>.
- . ‘Communication from the Commission to the European Parliament and the Council on the Evaluation of the European Network and Information Security Agency (ENISA)’, 1 June 2007. COM/2007/0285 final. <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52007DC0285>.
- . ‘Communication from the Commission to the European Parliament and the Council the Eu Internal Security Strategy in Action: Five Steps Towards a More Secure Europe’, 22 November 2010. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52010DC0673&qid=1683985600055>.
- . ‘Communication from the Commission to the European Parliament, the Council and the Committee of the Regions - Towards a General Policy on the Fight against Cyber Crime {SEC(2007) 641} {SEC(2007) 642}’, 22 May 2007. COM(2007) 267 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52007DC0267&qid=1684082047897>.
- . ‘COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - 5G for Europe: An Action Plan’, 14 September 2016. COM(2016) 588 final. [https://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=17131](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=17131).
- . ‘COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE



- COMMITTEE OF THE REGIONS - A Digital Single Market Strategy for Europe', 6 May 2015. COM(2015) 192 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN>.
- . 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Commission Provisions on "ARGUS" General Rapid Alert System', 2005. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52005DC0662&qid=1687593795069>.
- . 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Europe's Digital Competitiveness Report : Main Achievements of the I2010 Strategy 2005-2009 {SEC(2009) 1060} {SEC(2009) 1103} {SEC(2009) 1104}', 4 August 2009. COM/2009/0390 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52009DC0390&qid=1685802756502>.
- . 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Final Evaluation of the eEurope 2005 Action Plan and of the Multiannual Programme (2003-2006) for the Monitoring of eEurope 2005 Action Plan, Dissemination of Good Practices and the Improvement of Network and Information Security (Modinis)', 21 August 2009. COM/2009/0432 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52009DC0432&qid=1685698009806>.
- . 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Preparing Europe's Digital Future I2010 - Mid-Term Review {SEC(2008) 470}', 17 April 2008. COM/2008/0199 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52008DC0199&qid=1685802756502>.
- . 'COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry', 5 July 2016. COM/2016/0410 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0410>.
- . 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Agenda for Europe', 19 May 2010. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52010DC0245&qid=1683010781997>.
- . 'COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on Critical Information Infrastructure Protection "Achievements and next Steps: Towards Global Cyber-Security"', 31 March 2011. COM/2011/0163 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52011DC0163>.
- . 'COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on Critical Information Infrastructure Protection "Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience"', 30 March 2009. COM/2009/0149 final.

- <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52009DC0149>.
- . ‘COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the Mid-Term Review on the Implementation of the Digital Single Market Strategy A Connected Digital Single Market for All’, 10 May 2017. COM/2017/0228 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017DC0228>.
  - . ‘COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Secure 5G Deployment in the EU - Implementing the EU Toolbox’, 29 January 2020. COM/2020/50 final. <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2020:0050:FIN>.
  - . ‘COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Shaping Europe’s Digital Future’, 19 February 2020. COM/2020/67 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0067&qid=1641573209491>.
  - . ‘COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Tackling Online Disinformation: A European Approach’, 26 April 2018. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236>.
  - . ‘COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS The European Agenda on Security’, 28 April 2015. COM(2015) 185 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52015DC0185>.
  - . ‘Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - European Defence Action Plan’, 30 November 2016. COM/2016/0950 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016DC0950>.
  - . ‘Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy’, 24 July 2020. COM/2020/605 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0605>.
  - . ‘Communication from the Commission to the Spring European Council in Barcelona - The Lisbon Strategy - Making Change Happen’, 15 January 2002. COM/2002/0014 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52002DC0014>.
  - . ‘eEurope - An Information Society for All - Communication on a Commission Initiative for the Special European Council of Lisbon, 23 and 24 March 2000’, 8 December 1999. COM/99/0687 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:51999DC0687>.
  - . ‘eEurope - An Information Society for All - Progress Report for the Special European Council on Employment, Economic Reforms and Social Cohesion towards a Europe Based on Innovation and Knowledge Lisbon, 23 and 24 March 2000’, 8 March 2000.

- COM/2000/0130 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52000DC0130&qid=1685639413472>.
- . ‘eEurope 2002 - An Information Society for All - Draft Action Plan Prepared by the European Commission for the European Council in Feira - 19-20 June 2000’, 24 May 2000. COM (2000) 330 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52000DC0330>.
- . ‘EUROPE 2020 - A Strategy for Smart, Sustainable and Inclusive Growth’, 3 March 2010. COM/2010/2020 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52010DC2020>.
- . ‘Evaluation Study of Council Directive 2008/114 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection’, 2 April 2019. <https://op.europa.eu/en/publication-detail/-/publication/118dcd3d-b041-11ea-bb7a-01aa75ed71a1#>.
- . ‘Green Paper on a European Programme for Critical Infrastructure Protection’, 17 November 2005. COM/2005/0576 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52005DC0576>.
- . ‘Green Paper on the Convergence of the Telecommunications, Media and Information Technology Sectors, and the Implications for Regulation - Towards an Information Society Approach’, 3 December 1997. COM/97/0623 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A51997DC0623&qid=1684076807163>.
- . ‘Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services’, 16 October 1996. COM/96/0483 FINAL. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A51996DC0483&qid=1684518698752>.
- . ‘Growth, Competitiveness and Employment - White Paper Follow-Up’. Luxembourg, 1994.
- . ‘Information Technology Security Evaluation Criteria (ITSEC)’. Edited by Senior Officials Group - Information Systems Security. Department of Trade and Industry, 28 June 1991. <https://sogis.org/documents/itsec/itsec-en.pdf>.
- . ‘Information Technology Security Evaluation Manual (ITSEM)’. Edited by Senior Officials Group - Information Systems Security, 10 September 1993. <https://sogis.org/documents/itsec/itsem-en.pdf>.
- . ‘ITSEC Joint Interpretation Library (ITSEC JIL)’. Edited by Senior Officials Group - Information Systems Security, November 1998. <https://sogis.org/documents/itsec/ITSEC-JIL-V2-0-nov-98.pdf>.
- . ‘JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - Report on Implementation of the EU’s Cybersecurity Strategy for the Digital Decade’, 23 June 2021. JOIN 0166. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021JC0014>.
- . ‘JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU’, 13 September 2017. JOIN 450. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017JC0450>.
- . ‘JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - The EU’s Cybersecurity Strategy for the Digital Decade’, 16 December 2020. JOIN 18. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020JC0018>.

- . ‘JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Joint Framework on Countering Hybrid Threats a European Union Response’, 6 April 2016. JOIN/2016/018 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018>.
- . ‘JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace’, 7 February 2013. JOIN 1. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001>.
- . ‘JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Action Plan against Disinformation’, 5 December 2018. JOIN(2018) 36 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018JC0036&qid=1690703950858>.
- . ‘Proposal for a Council Decision Adopting a Multi-Annual Programme (2003-2005) for the Monitoring of eEurope, Dissemination of Good Practices and the Improvement of Network and Information Security (MODINIS)’, 26 November 2002. COM/2002/0425 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52002PC0425>.
- . ‘Proposal for a Council Decision in the Field of Information Security’, 13 September 1990. COM/90/314FINAL. OJ C 277, 5.11.1990, p. 18–24.
- . Proposal for a Council Decision on a Critical Infrastructure Warning Information Network (CIWIN) {SEC(2008)2701} {SEC(2008)2702} (2008). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52008PC0676&qid=1687594552943>.
- . Proposal for a Council framework Decision on combating terrorism (2001). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52001PC0521&qid=1691393731226>.
- . ‘Proposal for a COUNCIL RECOMMENDATION ON COMMON Information Technology Security Evaluation Criteria’, 10 September 1992. COM/92/298FINAL. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:51992PC0298>.
- . Proposal for a DIRECTIVE OF THE Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection {SEC(2006) 1648} {SEC(2006) 1654} (2006). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52006PC0787>.
- . Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents, Pub. L. No. 0109, COD (2023). [https://www.europarl.europa.eu/RegData/docs\\_autres\\_institutions/commission\\_eu\\_ropeenne/com/2023/0209/COM\\_COM\(2023\)0209\\_EN.pdf](https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_eu_ropeenne/com/2023/0209/COM_COM(2023)0209_EN.pdf).
- . Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the ‘EU Cybersecurity Agency’, and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (“Cybersecurity Act”), 2017/0225 (COD) § (2017). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0477>.
- . Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and

- amending Regulation (EU) 2019/1020 (Cybersecurity Resilience Act), 2022/0272(COD) § (2022). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0454>.
- . ‘Reflection Paper on the Future of European Defence’, 7 June 2017. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017DC0315>.
- . ‘REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)’, 18 April 2011. COM(2011) 225 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52011DC0225&qid=1685080832916>.
- . ‘Resolution on the Recommendation to the European Council: ‘Europe and the Global Information Society’ and the Communication from the Commission to the Council and the European Parliament and to the Economic and Social Committee and the Committee of the Regions: ‘Europe’ s Way to the Information Society: An Action Plan’’, 28 November 1994. COM(94)0347. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:51996IP0244>.
- . ‘ROADMAP - Proposal on a European Strategy for Internet Security’, November 2011.
- . ‘Towards a Dynamic European Economy, Green Paper on the Development of the Common Market for Telecommunications Services and Equipment’, 30 June 1987. COM/87/290FINAL. <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:51987DC0290>.
- European Data Protection Board. ‘Guidelines 9/2022 on Personal Data Breach Notification under GDPR’, 28 March 2023. [https://edpb.europa.eu/system/files/2023-04/edpb\\_guidelines\\_202209\\_personal\\_data\\_breach\\_notification\\_v2.0\\_en.pdf](https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf).
- European Data Protection Supervisor. ‘Second opinion on ePrivacy’, gennaio 2009. [https://edps.europa.eu/sites/edp/files/publication/09-01-09\\_epricacy\\_2\\_it.pdf](https://edps.europa.eu/sites/edp/files/publication/09-01-09_epricacy_2_it.pdf).
- European Defence Agency. ‘EDA’s Pooling & Sharing’, 30 January 2013. [https://eda.europa.eu/docs/default-source/eda-factsheets/final-p-s\\_30012013\\_factsheet\\_cs5\\_gris](https://eda.europa.eu/docs/default-source/eda-factsheets/final-p-s_30012013_factsheet_cs5_gris).
- ‘European Defence Fund (EDF) - Official Webpage of the European Commission. - European Commission’. Accessed 9 April 2024. [https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf-official-webpage-european-commission\\_en](https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf-official-webpage-european-commission_en).
- European Defence Matters*. ‘Eda’s Growing Role in Cybersecurity’. 2019.
- European Digital Rights. ‘Shadow Evaluation Report on the Data Retention Directive (2006/24/EC) 17 April 201’. Bruxelles: European Digital Rights, 17 April 2011. [https://edri.org/files/shadow\\_drd\\_report\\_110417.pdf](https://edri.org/files/shadow_drd_report_110417.pdf).
- European Network and Information Security Agency. ‘Cyber Incident Reporting in the EU - An Overview of Security Articles in EU Legislation’, August 2012. <https://www.enisa.europa.eu/publications/cyber-incident-reporting-in-the-eu/@@download/fullReport>.
- . ‘Technical Guideline on Incident Reporting under the EECR’, 22 March 2021. <https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc/@@download/fullReport>.
- European Parliament. ‘European Parliament Resolution of 3 October 2017 on the Fight against Cybercrime (2017/2068(INI))’, 3 October 2017. [https://www.europarl.europa.eu/doceo/document/TA-8-2017-0366\\_EN.pdf](https://www.europarl.europa.eu/doceo/document/TA-8-2017-0366_EN.pdf).
- . ‘European Parliament Resolution of 12 March 2019 on Security Threats Connected with the Rising Chinese Technological Presence in the EU and Possible Action on the

- EU Level to Reduce Them (2019/2575(RSP))', 12 March 2019. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019IP0156>.
- . 'European Parliament Resolution of 19 January 2016 on Towards a Digital Single Market Act', 19 January 2016. 2015/2147(INI). [https://www.europarl.europa.eu/doceo/document/TA-8-2016-0009\\_EN.pdf](https://www.europarl.europa.eu/doceo/document/TA-8-2016-0009_EN.pdf).
- . 'Proposal for a Regulation on Privacy and Electronic Communications | Legislative Train Schedule'. European Parliament, August 2023. <https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-e-privacy-reform>.
- . 'Resolution of Parliament of the 19th of May 2002 Calling for Legislative Measures Against High-Tech Crime', 19 May 2002.
- European Parliament and Council of the European Communities. Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions, 275 OJ L § (2000). <http://data.europa.eu/eli/dir/2000/46/oj/eng>.
- European Parliament and Council of the European Union. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046>.
- . Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, 024 OJ L § (1997). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31997L0066>.
- . Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Pub. L. No. 93, EC (1999). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0093>.
- . Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive), 108 OJ L § (2002). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0019>.
- . Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive), 108 OJ L § (2002). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0020>.
- . Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), 108 OJ L § (2002). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0021>.
- . Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive), 108 OJ L § (2002). <http://data.europa.eu/eli/dir/2002/22/oj/eng>.
- . Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Pub. L. No. 58, 201 OJ L (2002). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058>.

- . Directive 2009/43/EC of the European Parliament and of the Council of 6 May 2009 simplifying terms and conditions of transfers of defence-related products within the Community (Text with EEA relevance), 146 OJ L § (2009). <http://data.europa.eu/eli/dir/2009/43/oj/eng>.
- . Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC (Text with EEA relevance), 216 OJ L § (2009). <http://data.europa.eu/eli/dir/2009/81/oj/eng>.
- . Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance), Pub. L. No. 337, OJ L (2009). <http://data.europa.eu/eli/dir/2009/136/oj/eng>.
- . Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services, Pub. L. No. 337, OJ L (2009). <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32009L0140>.
- . Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, 335 OJ L § (2011). <http://data.europa.eu/eli/dir/2011/93/oj/eng>.
- . Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast), 321 OJ L § (2018). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L1972>.
- . Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), 333 OJ L § (2022). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555>.
- . Regulation (EC) No 1007/2008 of the European Parliament and of the Council of 24 September 2008 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration, 293 OJ L § (2008). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008R1007>.
- . Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, Pub. L. No. 1183, UE (2024). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1183>.
- . Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity

- at the institutions, bodies, offices and agencies of the Union, Pub. L. No. 2841 (2023). <http://data.europa.eu/eli/reg/2023/2841/oj/eng>.
- . Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004, 165 OJ L § (2013). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013R0526>.
- . Regulation (EU) No 580/2011 of the European Parliament and of the Council of 8 June 2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration Text with EEA relevance, 165 OJ L § (2011). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011R0580>.
- European Union Agency for Cybersecurity. ‘Guideline on Security Measures Under the EEECC’, 7 July 2021. <https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc/@@download/fullReport>.
- European Union Agency for Cybersecurity, Marnix Dekker, and Christoffer Karsberg. ‘Technical Guideline on Incident Reporting’, 24 October 2014. <https://www.enisa.europa.eu/publications/technical-guideline-on-incident-reporting/@@download/fullReport><https://www.enisa.europa.eu/publications/technical-guideline-on-incident-reporting/@@download/fullReport>.
- European Union Agency For Network And Information Security. ‘Forensic Analysis Network Incident Response Toolset, Document for Students’, December 2016. [https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material/documents/2016-resources/exe2\\_forensic\\_analysis\\_ii-toolset](https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material/documents/2016-resources/exe2_forensic_analysis_ii-toolset).
- . ‘Technical Guideline on Security Measures’, October 2014. [https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article\\_13a\\_ENISA\\_Technical\\_Guideline\\_On\\_Security\\_Measures\\_v2\\_0.pdf](https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf).
- ‘Executive Order -- Improving Critical Infrastructure Cybersecurity’, 12 February 2013. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.
- ‘Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of PersonalData’. Consiglio d’Europa, 10 October 2018. <https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a>.
- Falletta, Pietro. ‘Le Linee Guida Dell’Agenzia per l’Italia Digitale’. *Giornale Di Diritto Amministrativo*, no. 2 (2021): 163–71.
- Ferrari, Laura. ‘DDL Intelligenza Artificiale: La Società Civile Chiede Più Trasparenza e Tutela Dei Diritti’. *Agenda Digitale* (blog), 25 September 2024. <https://www.agendadigitale.eu/sicurezza/privacy/ddl-intelligenza-artificiale-la-societa-civile-chiede-piu-trasparenza-e-tutela-dei-diritti/>.
- Finocchiaro, Giusella. ‘Una Prima Lettura Del Reg. UE n. 910/2014 (c.d. “Eidas”): Identificazione “on Line”, Firme Elettroniche e Servizi Fiduciari (Reg. UE n. 910/2014)’. *Le Nuove Leggi Civili Commentate*, no. 3 (2015): 419–28.
- Floridi, Luciano. *Information: A Very Short Introduction*. Very Short Introductions 225. Oxford ; New York: Oxford University Press, 2010.
- . *Infosfera: etica e filosofia nell’età dell’informazione*. Digitalica. Torino: Giappichelli, 2009.



- . *La quarta rivoluzione: come l'infosfera sta trasformando il mondo*. Scienza e idee. Milano: Cortina Raffaello, 2017.
- . *The Onlife Manifesto: Being Human in a Hyperconnected Era*, 2014. <https://doi.org/10.1007/978-3-319-04093-6>.
- 'Foreign Information Manipulation and Interference (FIMI) and Cybersecurity'. Threat Landscape. European Union Agency for Cybersecurity, December 2022. <https://data.europa.eu/doi/10.2824/7501>.
- Franchina, Luisa. 'Le Infrastrutture Critiche e La Protezione Cibernetica Nazionale'. *Gnosis*, no. 4 (2013): 103–15.
- Franchina, Luisa, Andrea Lucariello, and Francesco Ressa. 'Ampliamento del perimetro di sicurezza nazionale cibernetica: ecco i settori di attività'. *Agenda Digitale*, 18 June 2021. <https://www.cybersecurity360.it/cybersecurity-nazionale/ampliamento-del-perimetro-di-sicurezza-nazionale-cibernetica-ecco-i-settori-di-attivita/>.
- Franchini, Marco. 'Alcune Considerazioni Sulle Nuove Competenze Del Comitato Parlamentare per La Sicurezza Della Repubblica'. *Rivista AIC*, no. 1 (2014): 12.
- Freni, Elisabetta. "'Golden Share": Raggiunta La Compatibilità Con l'ordinamento Comunitario?' *Giornale Di Diritto Amministrativo*, no. 1 (2013): 25–33.
- Friedewald, Michael, Ina Schiering, Nicholas Martin, and Dara Hallinan. 'Data Protection Impact Assessments in Practice: Experiences from Case Studies'. In *Computer Security. ESORICS 2021 International Workshops*, edited by Sokratis Katsikas, Costas Lambrinoudakis, Nora Cuppens, John Mylopoulos, Christos Kalloniatis, Weizhi Meng, Steven Furnell, et al., 13106:424–43. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2022. [https://doi.org/10.1007/978-3-030-95484-0\\_25](https://doi.org/10.1007/978-3-030-95484-0_25).
- Frosini, Tommaso Edoardo. 'L'ordine Giuridico Del Digitale'. *CERIDAP*, no. 2 (2023): 36–65.
- Frosini, Vittorio. 'La Libera Circolazione dei Beni e dei Servizi Informatici nel mercato comune europeo'. *Diritto dell'informazione e dell'informatica*, no. 1 (1995).
- Gellert, R. 'We Have Always Managed Risks in Data Protection Law'. *European Data Protection Law Review* 2, no. 4 (2016): 481–92. <https://doi.org/10.21552/EDPL/2016/4/7>.
- Gellert, Raphaël. 'Understanding the Notion of Risk in the General Data Protection Regulation'. *Computer Law & Security Review* 34, no. 2 (April 2018): 279–88. <https://doi.org/10.1016/j.clsr.2017.12.003>.
- Gianni, Francesca Di. 'Un'Europa "Ciberresiliente": La Risposta Dell'Unione Europea Alle Minacce e Agli Attacchi Informatici'. *Studi Sull'integrazione Europea*, no. 2 (2023): 399–424.
- Giupponi, Tommaso F. 'Il Governo Nazionale Della Cybersicurezza'. *Quaderni Costituzionali*, no. 2 (2024): 277–303.
- . 'La Corte e Il Segreto: Abu Omar, Ultimo Atto'. *Quaderni Costituzionali*, no. 2 (2014): 386–89.
- Goldsmith, Jack. 'Who Controls the Internet? Illusions of a Borderless World'. *Strategic Direction* 23, no. 11 (23 October 2007). <https://doi.org/10.1108/sd.2007.05623kae.001>.
- Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González., No. C-131/12 (European Court of Justice 13 May 2014).
- Grandis, Nicola. 'Agenzia per la cyber security, accelerare su tecnologia, investimenti e conoscenze: ecco perché'. *Agenda Digitale*, 5 July 2021. <https://www.cybersecurity360.it/cybersecurity-nazionale/agenzia-per-la-cyber->

- security-accelerare-su-tecnologia-investimenti-e-conoscenze-ecco-perche/.
- Grassi, Paul, Michael Garcia, and James Fenton. 'Digital Identity Guidelines'. National Institute of Standards and Technology, 2 March 2020. <https://doi.org/10.6028/NIST.SP.800-63-3>.
- Gual, Jordi. 'Regulation and the Development of Electronic Communications in Europe'. *Info* 4, no. 3 (2002): 42–49. <https://doi.org/10.1108/14636690210440004>.
- Guerrieri, Alessandra. *Regolazione e concorrenza nelle comunicazioni elettroniche*. Milano, [Padova]: Wolters Kluwer : CEDAM, 2021.
- Guida, Sergio. 'ENISA's Last Technical Analysis of Data Pseudonymization Advanced Measures in Data Protection and Privacy'. *European Journal of Privacy Law & Technologies*, no. 1 (2021): 262–74.
- Harašta, Jakub. 'Legally Critical: Defining Critical Infrastructure in an Interconnected World'. *International Journal of Critical Infrastructure Protection* 21 (June 2018): 47–56. <https://doi.org/10.1016/j.ijcip.2018.05.007>.
- 'Home | CVE'. Accessed 1 September 2023. <https://www.cve.org/>.
- Huang, Jingwei, and David M. Nicol. 'An Anatomy of Trust in Public Key Infrastructure'. *International Journal of Critical Infrastructures* 13, no. 2–3 (2017): 238–58. <https://doi.org/10.1504/IJCIS.2017.088234>.
- Iannuzzi, Antonio, and Francesco Laviola. 'I Diritti Fondamentali Nella Transizione Digitale Fra Libertà e Uguaglianza'. *Diritto Costituzionale*, no. 1 (2023): 9–40.
- Iannuzzi, Tino. 'La Corte Costituzionale è Il "Giudice Naturale" Della Autodichia. Nota Alla Sentenza Della Quinta Sezione Del Consiglio Di Stato n. 4150 Del 31 Maggio 2021'. *Federalismi.It*, no. 28 (2021): 58–75.
- Ibrido, Renato. '"In Direzione Ostinata e Contraria". La Risposta Della Corte Costituzionale Alla Dottrina Della Sindacabilità Dei Regolamenti Parlamentari'. *Rivista AIC*, no. 3 (2014): 3.
- Inter-Parliamentary Union. '146th Assembly and Related Meetings', 24 April 2024. <https://www.ipu.org/event/146th-assembly-and-related-meetings>.
- Inter-Parliamentary Union. 'Creating a Safe Cyberspace for Democracy', 24 April 2024. <https://www.ipu.org/event/creating-safe-cyberspace-democracy>.
- Inter-Parliamentary Union, Geneva Centre for Security Policy, Parliamentarians for Global Action, Parliamentarians for Nuclear Non-proliferation and Disarmament, Parliamentary Forum on Small Arms and Light Weapons, and World Future Council. 'Parliamentary Handbook on Implementation of Securing Our Common Future, the UN Secretary-General's Disarmament Agenda', 2020. [https://disarmamenthandbook.org/wp-content/uploads/2021/01/disarmament-handbook-2020\\_v07.pdf](https://disarmamenthandbook.org/wp-content/uploads/2021/01/disarmament-handbook-2020_v07.pdf).
- ISACA. 'How to Write Strong Risk Scenarios and Statements'. Accessed 12 November 2023. <https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-31/how-to-write-strong-risk-scenarios-and-statements>.
- ISC2. 'ISC2 Cybersecurity Workforce Study 2023', 2023. [https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2\\_Cybersecurity\\_Workforce\\_Study\\_2023.pdf?rev=52055d08ca644293bd7497725bb7fcb4](https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=52055d08ca644293bd7497725bb7fcb4).
- Juncker, Jean-Claude. 'A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change - Political Guidelines for the next European Commission', 15 July 2014. <https://commission.europa.eu/system/files/2019-09/juncker-political->

- guidelines-speech\_en.pdf.
- . ‘Speech by President Jean-Claude Juncker - State of the Union Address 2017’, 13 September 2017. [https://ec.europa.eu/commission/presscorner/api/files/document/print/en/speech\\_17\\_3165/SPEECH\\_17\\_3165\\_EN.pdf](https://ec.europa.eu/commission/presscorner/api/files/document/print/en/speech_17_3165/SPEECH_17_3165_EN.pdf).
- Kaiser, Elena. ‘The New NIS II Directive and Its Impact on Small and Medium Enterprises (SMEs): Initial Considerations’. *MediaLaws*, no. 1 (2023): 343–57.
- Kleinwächter, Wolfgang. ‘Wanted: Nobel Peace Prize Winners Who Create Peace in Cyberspace’. *Rivista Italiana Di Informatica e Diritto*, no. 1 (2022): 1\_25-29.
- Klimburg, Alexander and NATO Cooperative Cyber Defence Centre of Excellence. *National Cyber Security Framework Manual*. Tallinn, Estonia: NATO Cooperative Cyber Defense Center of Excellence, 2012. <http://ccdcoe.org/369.html>.
- Knieps, Günter. ‘Regulatory Reform of European Telecommunications: Past Experience and Forward-Looking Perspectives’. *European Business Organization Law Review* 2, no. 3–4 (2001): 641–55. <https://doi.org/10.1017/S1566752900000653>.
- Koh, Harold Hongju, Abram Chayes, Antonia Handler Chayes, and Thomas M. Franck. ‘Why Do Nations Obey International Law?’ *The Yale Law Journal* 106, no. 8 (June 1997): 2599. <https://doi.org/10.2307/797228>.
- Labriola, S. *Le Informazioni per La Sicurezza Dello Stato*. Milano, Italy, 1978.
- Labriola, Silvano. ‘Informazioni per La Sicurezza e Segreto Di Stato.’ *Diritto e Società* 2, no. 4 (1981): 833–59.
- Landler, Mark, and John Markoff. ‘Digital Fears Emerge After Data Siege in Estonia’. *The New York Times*, 29 May 2007, sec. Technology. <https://www.nytimes.com/2007/05/29/technology/29estonia.html>.
- Lazarou, Elena, Ionel Zamfir, Beatrix Immenkamp, Issam Hallak, Eric Pichon, Matthew Parry, and Branislav Stanicek. ‘Peace and Security in 2022 - Overview of EU Action and Outlook for the Future’. European Parliamentary Research Service, July 2022. [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/733605/EPRS\\_STU\(2022\)733605\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/733605/EPRS_STU(2022)733605_EN.pdf).
- Lazzaro, Anna. ‘Informazione e Comunicazione Digitale Nel Processo Di Modernizzazione Della Pubblica Amministrazione’. *MediaLaws - Law and Policy of the Media in a Comparative Perspective*, no. 2 (2018): 11.
- Lepore, Domenico. *Deming and Goldratt : The Theory of Constraints and the System of Profound Knowledge : The Decalogue*. Great Barrington, MA : North River Press, 1999. <http://archive.org/details/deminggoldratth0000lepo>.
- ‘L’esonazione Totale dalla Giurisdizione: Immunità dei Capi di Stato e Insindacabilità Parlamentare’. In *Le immunità della politica contributo allo studio delle prerogative costituzionali*, 139–203. Torino: G. Giappichelli, 2005.
- Longo, Erik. ‘Audizione Informale per Il Disegno Di Legge in Materia Di “Disposizioni in Materia Di Rafforzamento Della Cybersicurezza Nazionale e Di Reati Informatici” (AC 1717). Camera Dei Deputati, Commissioni Riunite I e II - Roma, 28 Marzo 2024’. *Rivista Italiana Di Informatica e Diritto*, no. 1 (2024): 65–70.
- . ‘“Digital Services Act” - Libertà Di Informazione. Libertà Di Informazione e Lotta Alla Disinformazione Nel “Digital Services Act”’. *Giornale Di Diritto Amministrativo*, no. 6 (2023): 737–45.
- Longo, Erik, and Andrea Pin. ‘Oltre Il Costituzionalismo? Nuovi Principi e Regole Costituzionali per l’era Digitale’. *Diritto Pubblico Comparato Ed Europeo*, no. 1 (2023): 103–16.

- Lorè, Filippo, and Paolo Musacchio. ““Cybersecurity” e Protezione Dei Dati Personali Ai Tempi Dell’“accountability”: Verso Un Cambio Di Prospettiva?” *Amministrativ@mente*, no. 1 (2021): 65–90.
- Lourenço, Marco, and Louis Marinos. ‘ENISA THREAT LANDSCAPE FOR 5G NETWORKS - Threat Assessment for the Fifth Generation of Mobile Telecommunications Networks (5G)’. ENISA Threat Landscape. 5G Networks. European Union Agency for Cybersecurity, November 2019. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks/@download/fullReport>.
- Lupo, Nicola. ‘Sull’autodichia La Corte Costituzionale, Dopo Lunga Attesa, Opta per La Continuità (Nota a Corte Cost. n. 262 Del 2017)’. *Forumcostituzionale.It* (blog), dicembre 2017. [https://www.forumcostituzionale.it/wordpress/wp-content/uploads/2017/11/nota\\_262\\_2017\\_lupo.pdf](https://www.forumcostituzionale.it/wordpress/wp-content/uploads/2017/11/nota_262_2017_lupo.pdf).
- Lynskey, Orla. ‘The Data Retention Directive Is Incompatible with the Rights to Privacy and Data Protection and Is Invalid in Its Entirety: Digital Rights Ireland’. *Common Market Law Review* 51, no. 6 (2014): 1789–1811.
- Macenaite, Milda. ‘The “Riskification” of European Data Protection Law through a Two-Fold Shift’. *European Journal of Risk Regulation* 8, no. 3 (September 2017): 506–40. <https://doi.org/10.1017/err.2017.40>.
- Marini-Balestra, Federico. *Manuale di diritto europeo e nazionale delle comunicazioni elettroniche*. Padova: CEDAM, 2013.
- Marinos, Louis, Adrian Belmonte Martin, Evangelos Rekleitis, George Spanoudakis, and Nikolaos Petroulakis. ‘Threat Landscape and Good Practice Guide for Software Defined Networks/5G’. Threat Landscape. European Union Agency for Cybersecurity, December 2015. <https://www.enisa.europa.eu/publications/sdn-threat-landscape/@download/fullReport>.
- Mario, Monti. ‘Speech by Mario MONTI - European Commissioner for the Single Market - Electronic Commerce in Europe - Creating a Favourable Environment for Electronic Commerce’, 8 July 1997. SPEECH/97/157. [https://ec.europa.eu/commission/presscorner/detail/en/SPEECH\\_97\\_157](https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_97_157).
- Markopoulou, Dimitra, Vagelis Papakonstantinou, and Paul De Hert. ‘The New EU Cybersecurity Framework: The NIS Directive, ENISA’s Role and the General Data Protection Regulation’. *Comput. Law Secur. Rev.* 35 (2019): 105336. <https://doi.org/10.1016/J.CLSR.2019.06.007>.
- Marrani, Daniela. ‘Cybersicurezza e Tutela Della Riservatezza Dei Dati Personali: Le Decisioni “Breyer” e “Tele2 Sverige” c. “Watson” Della Corte Di Giustizia UE’. *Il Diritto Dell’Unione Europea*, no. 4 (2017): 791–827.
- . ‘Il Coordinamento Delle Politiche per La “Cybersecurity” Dell’UE Nello Spazio Di Libertà, Sicurezza e Giustizia’. *Freedom, Security & Justice: European Legal Studies*, no. 1 (2021): 77–98.
- Martines, Francesco. ‘La Digitalizzazione Della Pubblica Amministrazione’. *MediaLaws*, no. 2 (2018): 10.
- Mason, P.J. ‘Ensuring Network Integrity’. In *IEE Colloquium on How to Compete and Connect: Understanding the Engineering of Telecommunications Network Interconnection*, 11/1-11/7, 1997. <https://doi.org/10.1049/ic:19970969>.
- Massera, A., and C. Mosca. ‘I servizi di informazione’. In *Trattato di diritto amministrativo, pt. spec.*, edited by S. Cassese, Vol. I. Milano, Italy, 2003.
- Matassa, Manfredi. ‘Una Strategia Nazionale a Difesa Del Cyberspazio’. *P.A. Persona e*

- Amministrazione*, no. 2 (2022): 625–53.
- Mattarella, Andrea. ‘Il “Cybercrime” Nell’ordinamento Italiano e Le Nuove Prospettive Dell’Unione Europea e Delle Nazioni Unite’. *Diritto Penale e Processo*, no. 6 (2022): 809–29.
- Mauriello, Luciano. ‘Libertà, Attività Informativa e Sicurezza Dello Stato.’ *Nuova Rassegna Di Legislazione, Dottrina e Giurisprudenza*, no. 15–16 (1987): 1579–96.
- Maurino, Marta. ‘“Cybersecurity”, Sicurezza Nazionale e Trattamento Dei Dati Personali’. *Amministrativamente*, no. 2 (2023): 939–72.
- McTaggart, Craig. ‘A Layered Approach to Internet Legal Analysis’. *McGill Law Journal* 48 (2003): 571.
- Merete Hagen, Janne, Eirik Albrechtsen, and Jan Hovden. ‘Implementation and Effectiveness of Organizational Information Security Measures’. *Information Management & Computer Security* 16, no. 4 (10 October 2008): 377–97. <https://doi.org/10.1108/09685220810908796>.
- Mishra, Sushma. ‘Organizational Objectives for Information Security Governance: A Value Focused Assessment’. *Information & Computer Security* 23, no. 2 (8 June 2015): 122–44. <https://doi.org/10.1108/ICS-02-2014-0016>.
- ‘Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data’. Consiglio d’Europa, 18 May 2018. [https://search.coe.int/cm/Pages/result\\_details.aspx?ObjectId=09000016807c65bf](https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf).
- Montanaro, Federica. ‘Il Bisogno Di Sicurezza Sulla Rete: L’intervento Penale Italiano Ed Europeo’. *La Legislazione Penale*, no. 3 (2022): 3–14.
- Mónton, V. ‘Risk Assessment Methodology for Network Integrity’. *BT Technology Journal* 15, no. 1 (1 January 1997): 223–34. <https://doi.org/10.1023/A:1018664103282>.
- Moro, Paolo. ‘Macchine come noi. Natura e limiti della soggettività robotica’. In *Intelligenza artificiale: il diritto, i diritti, l’etica*, by Guido Alpa and Augusto Barbera, 45–61. edited by Ugo Ruffolo. Tech e-Law. Milano: Giuffrè Francis Lefebvre, 2020.
- Moroni, Lorenzo. ‘La Governance Della Cybersicurezza a Livello Interno Ed Europeo: Un Quadro Intricato’. *Federalismi.It*, no. 14 (2024): 179–97.
- Mortati, Costantino, Franco Modugno, Antonio Baldassarre, and Carlo Mezzanotte. *Istituzioni di diritto pubblico*. 10a ed. Manuali di scienze giuridiche. Padova: CEDAM, 1991.
- Mounier, Gregory. ‘Europol: A New Player in the EU External Policy Field?’ *Perspectives on European Politics and Society* 10, no. 4 (December 2009): 582–602. <https://doi.org/10.1080/15705850903314841>.
- Nannipieri, Lorenzo. ‘Cybersicurezza e Appalti Pubblici: Verso Un Nuovo (e Incerto) Quadro Regolatorio’. *Rivista Italiana Di Informatica e Diritto*, no. 1 (2024): 19–23.
- National Cyber Security Centre. ‘Cyber Essentials: Requirements for IT Infrastructure v3.1’, April 2023. <https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf>.
- National Institute of Standards and Technology. ‘Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1’. Gaithersburg, MD: National Institute of Standards and Technology, 16 April 2018. <https://doi.org/10.6028/NIST.CSWP.04162018>.
- National Institute of Standards and Technology. ‘Nist Privacy Framework:: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0’. Gaithersburg, MD: National Institute of Standards and Technology, 16 January 2020. <https://doi.org/10.6028/NIST.CSWP.01162020>.

- . ‘The NIST Cybersecurity Framework 2.0’. Gaithersburg, MD: National Institute of Standards and Technology, 26 February 2024. <https://doi.org/10.6028/NIST.CSWP.29>.
- Nava, Marco. *Regolamentazione e contenzioso tra operatori nelle comunicazioni elettroniche*. Torino: Giappichelli, 2012.
- ‘NCP - Information’. Accessed 26 November 2023. <https://ncp.nist.gov/general>.
- NIS Cooperation Group. ‘Cybersecurity of 5G Networks EU Toolbox of Risk Mitigating Measures’, January 2020.
- . ‘EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks’. NIS Cooperation Group, 9 October 2019. [https://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=62132](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132).
- . ‘Identification of Operators of Essential Services Reference Document on Modalities of the Consultation Process in Cases with Cross-Border Impact - CG Publication 07/2018’, July 2018. [https://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=53661](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53661).
- . ‘Reference Document on Incident Notification for Operators of Essential Services - Circumstances of Notification - CG Publication 02/2018’, February 2018. [https://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=53644](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53644).
- . ‘Reference Document on Security Measures for Operators of Essential Services - CG Publication 01/2018’, February 2018. [https://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=53643](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53643).
- . ‘Report on Member States’ Progress in Implementing the EU Toolbox on 5G Cybersecurity’. NIS Cooperation Group, July 2020. [https://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=68510](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68510).
- . ‘Second Report on Member States’ Progress in Implementing the EU Toolbox on 5G Cybersecurity’. NIS Cooperation Group, June 2023. <https://ec.europa.eu/newsroom/dae/redirection/document/96519>.
- NIST. ‘Introduction to the Framework Roadmap’, 13 April 2018. <https://www.nist.gov/cyberframework/online-learning/introduction-framework-roadmap>.
- NIST. ‘National Institute of Standards and Technology’. Text, 20 November 2023. <https://www.nist.gov/>.
- Nora, Simon, and Alain Minc. ‘L’informatisation de la société rapport a M.le Président de la République’. Paris, January 1978. [https://medias.vie-publique.fr/data\\_storage\\_s3/rapport/pdf/154000252.pdf](https://medias.vie-publique.fr/data_storage_s3/rapport/pdf/154000252.pdf).
- ‘Normativa Di Riferimento - Sistema Di Informazione per La Sicurezza Della Repubblica’. Accessed 1 January 2024. <https://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento.html>.
- Notarmuzi, Carlo. ‘DigitPA: La Terza Riorganizzazione Dell’informatica Pubblica’. *Giornale Di Diritto Amministrativo*, no. 10 (2010): 1014–20.
- ‘NVD - Vulnerability Status’. Accessed 1 September 2023. <https://nvd.nist.gov/vuln/vulnerability-status>.
- Orofino, Marco. *Profili costituzionali delle comunicazioni elettroniche nell’ordinamento multilivello*. Collana diritto pubblico 26. Milano: Giuffrè, 2008.
- Pace, Alessandro. ‘Stato Costituzionale e Segreto Di Stato: Una Coesistenza Problematica’. *Giurisprudenza Costituzionale*, no. 5 (2015): 1719–37.
- Pallieri, Balladore. *Diritto costituzionale*. Giuffrè., 1953.

- Palmieri, Antonio. 'Intelligenza artificiale ed operazioni di trattamento dei dati personali'. // *Foro italiano*, no. 3 (2023): 210–12.
- Parcu, Pier Luigi, and Virginia Silvestri. 'Electronic Communications Regulation in Europe: An Overview of Past and Future Problems'. *Utilities Policy* 31, no. C (2014): 246–55. <https://doi.org/10.1016/j.jup.2014.03.009>.
- Petersen, Peter B. 'Total Quality Management and the Deming Approach to Quality Management'. *Journal of Management History* 5, no. 8 (1 January 1999): 468–88. <https://doi.org/10.1108/13552529910290520>.
- Petersen, Rodney, Danielle Santos, Karen Wetzel, Matthew Smith, and Gregory Witte. 'Workforce Framework for Cybersecurity (NICE Framework)'. National Institute of Standards and Technology, 16 November 2020. <https://doi.org/10.6028/NIST.SP.800-181r1>.
- Pietroletti, Alessandra, and Alessandro Nicotra. 'Tutela Della Salute, Sistemi Digitali e Privacy'. *Rivista Italiana Di Informatica e Diritto*, no. 1 (2022): 2\_283-294.
- Pisa, Paolo. 'Il Segreto Di Stato Di Fronte Alla Corte Costituzionale: Luci Ed Ombre in Attesa Della "Riforma"'. *Giurisprudenza Costituzionale*, no. 8 (1977): 1206–14.
- Pizzetti, Federico Gustavo. 'Il Più Recente Orientamento Della Corte Costituzionale Nel Caso Abu Omar: Novità Sul Segreto Di Stato?' *Processo Penale e Giustizia*, no. 6 (2014): 13.
- Pizzetti, Franco. *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo*. Seconda ristampa. I diritti nella rete nella rete, 4.1. Torino: G. Giappichelli, 2016.
- Pizzetti, Franco <1946- >. *Privacy e il diritto europeo alla protezione dei dati personali. 2, Il regolamento europeo 2016/679*. I diritti nella rete della rete 4.2. Torino: Giappichelli, 2016.
- Poggiali, Barbara. 'Le Opportunità Dell'Intelligenza Artificiale per La Sicurezza'. *Gnosis*, no. 2 (2019): 135–41.
- Pohle, Julia, and Thorsten Thiel. 'Digital Sovereignty'. *Internet Policy Review* 9, no. 4 (17 December 2020). <https://doi.org/10.14763/2020.4.1532>.
- Poletti, Simone. 'La Sicurezza Cibernetica Nazionale Ed Europea, Alla Luce Della Creazione Del Perimetro Di Sicurezza Nazionale Cibernetica'. *MediaLaws*, no. 2 (2023): 398–410.
- Polis, Richard I. 'European Needs and Attitudes Towards Information Security'. *Cryptologia* 12, no. 4 (October 1988): 234–39. <https://doi.org/10.1080/0161-118891862981>.
- Pollicino, Oreste. 'Di Cosa Parliamo Quando Parliamo Di Costituzionalismo Digitale?' *Quaderni Costituzionali*, no. 3 (2023): 569–94.
- Pollitt, Mark. 'A History of Digital Forensics'. In *Advances in Digital Forensics VI*, edited by Kam-Pui Chow and Sujeet Sheno, 3–15. IFIP Advances in Information and Communication Technology. Berlin, Heidelberg: Springer, 2010. [https://doi.org/10.1007/978-3-642-15506-2\\_1](https://doi.org/10.1007/978-3-642-15506-2_1).
- Ponti, Benedetto. 'Il Rapporto Tra Cybersicurezza e Tutela Dei Dati Personali: Sinergie, Bilanciamenti e Parallelismi'. *Rivista Italiana Di Informatica e Diritto*, no. 2 (2024): 2.
- Presidente del Consiglio dei Ministri. 'DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 12 giugno 2009, n. 7/2009 - Determinazione dell'ambito dei singoli livelli di segretezza, dei soggetti con potere di classifica, dei criteri d'individuazione delle materie oggetto di classifica nonché dei modi di accesso nei luoghi militari o definiti di interesse per la sicurezza della Repubblica', 12 June 2009. <https://www.parlamento.it/documenti/repository/commissioni/bicamerali/COMITATO%20SICUREZZA/DPCM%2012%20GIUGNO%202009%20N.7.pdf>.

- Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA (2017). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52017PC0489>.
- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent, and amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No 1211/2009 and (EU) No 531/2012 (2013). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013PC0627>.
- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters (2018). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:225:FIN>.
- Prossomariti, Roberto. 'Riflessioni Sul Segreto Di Stato a Partire Dal Caso Abu Omar: Quali Prospettive Dopo La Condanna Di Strasburgo?' *Costituzionalismo.It*, no. 1 (2016): 4.
- Public Law 113 - 274 - Cybersecurity Enhancement Act of 2014, Pub. L. No. 274, 274 (2014). <https://www.govinfo.gov/app/details/PLAW-113publ274>.
- Pursiainen, Christer. 'The Challenges for European Critical Infrastructure Protection'. *Journal of European Integration* 31, no. 6 (1 November 2009): 721–39. <https://doi.org/10.1080/07036330903199846>.
- Qi, Aimin, Guosong Shao, and Wentong Zheng. 'Assessing China's Cybersecurity Law'. *Computer Law & Security Review* 34 (1 September 2018). <https://doi.org/10.1016/j.clsr.2018.08.007>.
- Quelle, C. 'The "Risk Revolution" in EU Data Protection Law: We Can't Have Our Cake and Eat It, Too'. *Cybersecurity*, 11 July 2017. <https://www.semanticscholar.org/paper/The-%E2%80%98Risk-Revolution%E2%80%99-in-EU-Data-Protection-Law%3A-We-Quelle/4bd00e31cb2965ba67c5471e4f02573e2db4c5dd>.
- Quinn, Stephen D, Murugiah Souppaya, Melanie Cook, and Karen Scarfone. 'National Checklist Program for IT Products - Guidelines for Checklist Users and Developers'. Gaithersburg, MD: National Institute of Standards and Technology, February 2018. <https://doi.org/10.6028/NIST.SP.800-70r4>.
- Raffiotta, Edoardo. 'Cybersecurity Regulation in the European Union and the Issues of Constitutional Law'. *Rivista AIC*, no. 4 (30 September 2022). [https://www.rivistaaic.it/images/rivista/pdf/4\\_2022\\_01\\_Raffiotta.pdf](https://www.rivistaaic.it/images/rivista/pdf/4_2022_01_Raffiotta.pdf).
- Raffiotta, Edoardo C. 'Dalla "Self-Regulation" Alla "over-Regulation" in Ambito Digitale: Come (e Perché) Di Un Necessario Cambio Di Prospettiva'. *Osservatorio Sulle Fonti*, no. 2 (2023): 245–67.
- Ramadhan, Iqbal. 'ASEAN-China Cybersecurity Cooperation: Challenges and Opportunities'. *Journal of Social and Political Sciences* 6 (27 October 2023): 1–10. <https://doi.org/10.31014/aior.1991.06.04.440>.
- Rashid, Awais, Howard Chivers, Emil Lupu, Andrew Martin, and Steve Schneider, eds. *CyBOK - The Cyber Security Body of Knowledge*. 1.1.0., 2021. [https://www.cybok.org/media/downloads/CyBOK\\_v1.1.0.pdf](https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf).
- Rauhofer, Judith, and Daithí Mac Síthigh. 'The Data Retention Directive Never Existed'. *SCRIPTed* 11, no. 1 (2014). <https://doi.org/10.2966/scrip.110114.118>.
- Razzante, Ranieri. 'L'attribuzione Degli Attacchi Informatici'. *European Journal of Privacy Law*



- & *Technologies*, no. 2 (2022): 0\_215-241.
- Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office (Text with EEA relevance), 337 OJ L § (2009). <http://data.europa.eu/eli/reg/2009/1211/oj/eng>.
- Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (Text with EEA relevance), 310 OJ L § (2015). <http://data.europa.eu/eli/reg/2015/2120/oj/eng>.
- Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council Text with EEA relevance, 316 OJ L § (2012). <http://data.europa.eu/eli/reg/2012/1025/oj/eng>.
- Renda, Kadri Kaan. 'THE DEVELOPMENT OF EU CYBERSECURITY POLICY: FROM A COORDINATING ACTOR TO A CYBER POWER?' *Ankara Avrupa Calismalari Dergisi*, 2022.
- Renzi, Andrea. 'La Sicurezza Cibernetica: Lo Stato Dell'arte'. *Giornale Di Diritto Amministrativo*, no. 4 (2021): 538–48.
- Research Center of Cyber Intelligence and Information Security and CINI Cybersecurity National Lab Consorzio Interuniversitario Nazionale per l'Informatica. '2015 Italian Cyber Security Report', February 2016. [https://www.cybersecurityframework.it/sites/default/files/CSR2015\\_ENG.pdf](https://www.cybersecurityframework.it/sites/default/files/CSR2015_ENG.pdf).
- . '2015 Italian Cyber Security Report - Un Framework Nazionale per la Cyber Security', February 2016. [https://www.cybersecurityframework.it/sites/default/files/CSR2015\\_web.pdf](https://www.cybersecurityframework.it/sites/default/files/CSR2015_web.pdf).
- . '2016 Italian Cybersecurity Report - Controlli Essenziali di Cybersecurity', March 2017. <https://www.cybersecurityframework.it/sites/default/files/csr2016web.pdf>.
- . 'Framework Nazionale per La Cybersecurity e La Data Protection', February 2019. [https://www.cybersecurityframework.it/sites/default/files/framework2/Framework\\_nazionale\\_cybersecurity\\_data\\_protection.pdf](https://www.cybersecurityframework.it/sites/default/files/framework2/Framework_nazionale_cybersecurity_data_protection.pdf).
- Resta, Federica. 'Cybersicurezza e Protezione Dati: Un Rapporto Ambivalente'. *Rivista Italiana Di Informatica e Diritto*, no. 2 (2024): 1.
- RHC, Redazione. 'Attacco informatico al Consiglio Superiore della Magistratura. Attivo il geolocking ma non una soluzione definitiva'. il blog della sicurezza informatica, 20 April 2023. <https://www.redhotcyber.com/post/attacco-informatico-alla-consiglio-superiore-della-magistratura/>.
- Ridolfi, Melissa. 'Servizi Di Informazione e Cybersicurezza'. *Giornale Di Diritto Amministrativo*, no. 2 (2023): 207–11.
- Rodotà, Stefano. 'Privacy fra individuo e collettività'. *Politica del diritto*, 1974.
- Rodriguez Ayuso, Juan Francisco. 'Verso il raggiungimento di un mercato unico interno in materia di transazioni elettroniche. Il nuovo regolamento europeo 910/2014'. *Federalismi.it*, no. 24 (2017): 14.

- Romano, Bianca Nicla. 'Il Rischio Di "Attacchi" Ai Sistemi Informatici Tra Fattispecie Penalmente Rilevanti, Tutela Dei Dati Ed Esigenze Di "Buona Amministrazione"'. *Amministrativ@mente*, no. 3 (2021): 545–94.
- Rossa, Stefano. 'Administrative Law Reflections on Cybersecurity and on Its Institutional Actors, in the European Union and Italy'. *Italian Journal of Public Law*, no. 2 (2022): 426–50.
- Sabella, Pietro Maria. 'Il Fenomeno Del "Cybercrime" Nello Spazio Giuridico Contemporaneo. Prevenzione e Repressione Degli Illeciti Penali Connessi All'utilizzo Di Internet per Fini Di Terrorismo, Tra Esigenze Di Sicurezza e Rispetto Dei Diritti Fondamentali'. *Informatica e Diritto*, no. 1–2 (2017): 139–76.
- Sacco Ginevri, Andrea. 'I "Golden Powers" Dello Stato Nei Settori Strategici Dell'economia'. *Federalismi.It*, no. 22 (2016): 14.
- Salamone, Maria, and Di Luca Vincenzo. 'La Disciplina Del "Cyberspace" Alla Luce Della Direttiva Europea Sulla Sicurezza Delle Reti e Dell'informazione: Contesto Normativo Nazionale Di Riferimento, Ruolo Dell'"intelligence" e Prospettive "de Iure Condendo"'. *Federalismi.It*, no. 23 (2017): 8.
- Sandulli, Aldo Maria. 'Note Minime in Tema Di Segreto Di Stato'. *Giurisprudenza Costituzionale*, no. 8 (1977): 1200–1205.
- Santos, Marta Fernandes dos, and Alfonso Contaldo. 'L'agenzia per La Cybersicurezza Nazionale: Istituzione e Problematiche in Campo'. *Rivista Amministrativa Della Repubblica Italiana*, no. 5–6 (2022): 2\_343-365.
- Sardu, Alessandra. 'L'"international Cybersecurity Law": Lo Stato Dell'arte'. *La Comunità Internazionale*, no. 1 (2020): 5–42.
- Sarzana di S. Ippolito, Fulvio. *Comunicazioni elettroniche europee : Direttiva (UE) 2018/1972 5G, fibra, cybersecurity, concorrenza e tutela degli utenti*. IPSOA guida alle novità. Milano: Wolters Kluwer Italia, 2019.
- Sarzana Di Sant'Ippolito, Carlo. 'I Problemi Delle Infrastrutture Critiche Informatizzate'. *Diritto Dell'Internet*, no. 4 (2007): 331–34.
- Savino, Mario. 'Solo per i Tuoi Occhi? La Riforma Del Sistema Italiano Di Intelligence'. *Giornale Di Diritto Amministrativo*, no. 2 (2008): 121–31.
- Scaccia, Gino. '"Intelligence" e Segreto Di Stato Nella Legge n. 133 Del 2012'. *Diritto e Società*, no. 3 (2012): 585–600.
- Schjolberg, Stein, and Solange Ghernaouti-Helie. 'A Global Treaty on Cybersecurity and Cybercrime - Second Edition 2011', 2011.
- Schmitz-Berndt, Sandra, and Pier Giorgio Chiara. 'One Step Ahead: Mapping the Italian and German Cybersecurity Laws against the Proposal for a NIS2 Directive'. *International Cybersecurity Law Review* 3, no. 2 (1 December 2022): 289–311. <https://doi.org/10.1365/s43439-022-00058-7>.
- Schneider, Giulia. 'La Resilienza Operativa Digitale Come Materia Di "Corporate Governance": Prime Riflessioni a Partire Dal DORA'. *Corporate Governance*, no. 4 (2022): 553–80.
- Sciolino, Elaine. 'Spain Struggles to Absorb Worst Terrorist Attack in Its History'. *The New York Times*, 11 March 2004, sec. World. <https://www.nytimes.com/2004/03/11/international/europe/spain-struggles-to-absorb-worst-terrorist-attack-in-its.html>.
- Selamat, Siti Rahayu, Y. Robiah, and Shahrin Sahib. 'Mapping Process of Digital Forensic Investigation Framework' 8 (1 January 2008).
- Senato della Repubblica. 'Mozioni 23 maggio 2012, n. 1-00405 e n. 1-00491', 23 May 2012.

- [https://www.sicurezzacibernetica.it/db/\[2012\]%20Mozioni%2023%20maggio%202012,%20n.%201-00405%20e%20n.%201-00491%20-%20Mozioni%20sulla%20sicurezza%20da%20minaccia%20cibernetica.pdf](https://www.sicurezzacibernetica.it/db/[2012]%20Mozioni%2023%20maggio%202012,%20n.%201-00405%20e%20n.%201-00491%20-%20Mozioni%20sulla%20sicurezza%20da%20minaccia%20cibernetica.pdf).
- Serini, Federico. 'Il Sistema Europeo Di Cooperazione Informativa per Il Contrasto Alle Minacce Informatiche. Verso Una Definizione Di Cybersicurezza Integrata?' *MediaLaws*, no. 3 (2023): 144–87.
- . 'La Frammentazione Del Cyberspazio Merceologico Tra Certificazioni e Standard Di Cybersicurezza. Alcune Considerazioni Alla Luce Delle Discipline Europea e Italiana'. *Rivista Italiana Di Informatica e Diritto*, no. 2 (2023): 41–76.
- . 'La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021'. *Federalismi.it*, no. 12 (20 April 2022).
- Sica, Tommaso. "Cybersecurity" e Governo Del Rischio'. *Corporate Governance*, no. 4 (2022): 581–94.
- Sieber, Ulrich. 'Legal Aspects of Computer-Related Crime in the Information Society (COMCRIME Study)'. University of Würzburg, April 1998.
- Simoncini, Andrea. 'La Co-Regolazione Delle Piattaforme Digitali'. *Rivista Trimestrale Di Diritto Pubblico*, no. 4 (2022): 1031–49.
- Stelo, Vittorio. 'Così è Cambiata l'Intelligence in Italia'. *Gnosis*, no. 4 (2007). <https://gnosis.aisi.gov.it/Gnosis/Rivista13.nsf/ServNavig/59>.
- Sterpa, Alessandro. 'L'ordine giuridico dell'algoritmo: un nuovo ordinamento giuridico'. In *L'ordine giuridico dell'algoritmo*, 9–31. Tiresia - Future Studies and Law 1. Naples: Editoriale Scientifica, 2024. [https://editorialescientifica.it/wp-content/uploads/2024/04/Open-access-Sterpa\\_Lordine-giuridico-dellalgoritmo.pdf](https://editorialescientifica.it/wp-content/uploads/2024/04/Open-access-Sterpa_Lordine-giuridico-dellalgoritmo.pdf).
- Stringhi, Elisabetta. 'La Minaccia Del "Deepfake" Ed i Rischi per La "Cybersecurity" Delle Organizzazioni Economiche: Un Approccio Pratico'. *Cyberspazio e Diritto*, no. 1 (2021): 59–77.
- Suzana, Elena, and Izabela Cristina Bacian. 'Implementation of the Lisbon Treaty Provisions on the Common Security and Defence Policy (CSDP)'. Briefing. European Parliamentary Research Service, February 2016. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/573285/EPRS\\_BRI\(2016\)573285\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/573285/EPRS_BRI(2016)573285_EN.pdf).
- Sviatun, Olena V., Olga V. Goncharuk, Chernysh Roman, Olena Kuzmenko, and Ihor V. Kozych. 'Combating Cybercrime: Economic and Legal Aspects'. *Wseas Transactions on Business and Economics* 18 (2021). <https://doi.org/10.37394/23207.2021.18.72>.
- 'Sweden Admits Lisbon Agenda "failure" | EurActiv', 3 June 2009. <http://web.archive.org/web/20110609124031/http://www.euractiv.com/en/priorities/sweden-admits-lisbon-agenda-failure/article-182797>.
- Tabassi, Elham. 'Artificial Intelligence Risk Management Framework (AI RMF 1.0)'. *NIST*, 26 January 2023. <https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-ai-rmf-10>.
- Tabellini, Guido, and Charles Wyplosz. 'Supply-Side Reforms in Europe: Can the Lisbon Strategy Be Repaired?' *Swedish Economic Policy Review* 1, no. 13 (2006): 101–56.
- 'The Global Risks Report 2023'. Insight Report. World Economic Forum, January 2023.
- 'The Modernised Convention 108: Novelties in a Nutshell'. Consiglio d'Europa, 2018. <https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8>.
- Timmers, Paul. 'The European Union's Cybersecurity Industrial Policy'. *Journal of Cyber Policy* 3, no. 3 (2 September 2018): 363–84.

- <https://doi.org/10.1080/23738871.2018.1562560>.
- Tirino, Nazzareno. 'Segreto di Stato e conflitto di attribuzione fra poteri dello Stato'. *dirittifondamentali.it*, no. 1 (2016). [http://dirittifondamentali.it/wp-content/uploads/2019/04/1\\_2016-tirino\\_segreto-di-stato-e-conflitto-di-attribuzione-fra-poteri-dello-stato.pdf](http://dirittifondamentali.it/wp-content/uploads/2019/04/1_2016-tirino_segreto-di-stato-e-conflitto-di-attribuzione-fra-poteri-dello-stato.pdf).
- Tracey, Sarah. 'The Fall of the Data Retention Directive'. *Communications Law* 20, no. 2 (2015): 53–55.
- Tracol, Xavier. 'Legislative Genesis and Judicial Death of a Directive: The European Court of Justice Invalidated the Data Retention Directive (2006/24/EC) Thereby Creating a Sustained Period of Legal Uncertainty about the Validity of National Laws Which Enacted It'. *Computer Law & Security Review* 30, no. 6 (2014): 736–46. <https://doi.org/10.1016/j.clsr.2014.09.008>.
- Traynor, Ian. 'Russia Accused of Unleashing Cyberwar to Disable Estonia'. *The Guardian*, 17 May 2007, sec. World news. <https://www.theguardian.com/world/2007/may/17/topstories3.russia>.
- UN General Assembly. 'Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures :: Resolution /: Adopted by the General Assembly'. UN, 30 January 2004. <https://digitallibrary.un.org/record/509571>.
- United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union, No. Case C-66/04 (ECJ 6 December 2005).
- United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union, No. Case C-217/04 (ECJ 2 May 2006).
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (usa Patriot Act) Act of 2001, Pub. L. No. 107–56 (2001). <https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf>.
- UPC DTH Sàrl contro Nemzeti Média- és Hírközlési Hatóság Elnöksége, No. C-475/12 (European Court of Justice 30 April 2014).
- Vanegas, Juan Sebastien. 'La Violazione Dei Requisiti Di Sicurezza Informatica Di Cui All'articolo 32 Del GDPR'. *Rivista Italiana Di Informatica e Diritto*, no. 2 (2020): 5–14.
- Viganò, Eleonora, Michele Loi, and Emad Yaghmaei. 'Cybersecurity of Critical Infrastructure'. In *The Ethics of Cybersecurity*, edited by Markus Christen, Bert Gordijn, and Michele Loi, 157–77. The International Library of Ethics, Law and Technology. Cham: Springer International Publishing, 2020. [https://doi.org/10.1007/978-3-030-29053-5\\_8](https://doi.org/10.1007/978-3-030-29053-5_8).
- Vigna, Piero Luigi. 'La Nuova Disciplina Dei Servizi Di Sicurezza'. *La Legislazione Penale*, no. 4 (2007): 693–702.
- Viviani, A. *Servizi Segreti Italiani 1815/1985*. Roma, Italy, 1985.
- Warren, Adam, Robin Bayley, Colin Bennett, Andrew Charlesworth, Roger Clarke, and Charles Oppenheim. 'Privacy Impact Assessments: International Experience as a Basis for UK Guidance'. *Computer Law & Security Review* 24, no. 3 (January 2008): 233–42. <https://doi.org/10.1016/j.clsr.2008.03.003>.
- Warren, Samuel D., and Louis D. Brandeis. 'The Right to Privacy'. *Harvard Law Review* 4, no. 5 (15 December 1890): 193–220.
- Watney, Murdoch. 'The Way Forward in Addressing Cybercrime Regulation on a Global Level'. *Journal of Internet Technology and Secured Transaction* 1, no. 3 (1 September 2012): 61–67. <https://doi.org/10.20533/jitst.2046.3723.2012.0009>.
- Weiss, Marie-Andrée. 'Towards Mandatory Data Breach Notification Laws in the European Union'. *Journal of Internet Law* 14, no. 12 (2011): 24–29.

- Wessel, Ramses A. 'Cybersecurity in the European Union: Resilience through Isolation?' In *The Routledge Handbook of European Security Law and Policy*, by Zhaklin V. Yaneva and Marzia Scopelliti, 283–300. edited by E. Conde, 1st ed. London ; New York: Taylor and Francis, 2019. <https://doi.org/10.4324/9780429465918-18>.
- Wetter, Olive Emil. 'From Short-Term Goals to Organizational Objectives : Managing Security Control Using Goal Setting'. University of Zurich, 2012. <https://doi.org/10.5167/UZH-164118>.
- Woodward, Rachel. 'Establishing Europol'. *European Journal on Criminal Policy and Research* 1, no. 4 (December 1993): 7–33. <https://doi.org/10.1007/BF02249463>.
- Working Party Article 29. 'Guidelines on Personal Data Breach Notification under Regulation 2016/679'. WP29, Ottobre 2017. WP250rev.01.
- . 'Opinion 1/2009 on the Proposals Amending Directive 2002/58/EC on Privacy and Electronic Communications (e-Privacy Directive)'. WP29, 10 February 2009. WP159. [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp159\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp159_en.pdf).
- . 'Opinion 2/2008 on the Review of the Directive 2002/58/EC on Privacy and Electronic Communications (ePrivacy Directive)'. WP29, 15 May 2008. WP150. [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp150\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp150_en.pdf).
- . 'Opinion 3/2010 on the Principle of Accountability', 13 July 2010. WP173. [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf).
- . 'Opinion 03/2014 on Personal Data Breach Notification'. WP29, 25 March 2014. WP213.
- . 'Opinion 4/2007 on the Concept of Personal Data'. WP29, 20 June 2007. WP136. [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf).
- . 'Opinion 7/2000 On the European Commission Proposal for a Directive of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector of 12 July 2000 COM (2000) 385', 2 November 2000. WP36. [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp36\\_en.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp36_en.pdf).
- 'World Summit on the Information Society'. Accessed 17 June 2023. <https://www.itu.int/net/wsis/>.
- Wright, David. 'Should Privacy Impact Assessments Be Mandatory?' *Communications of the ACM* 54, no. 8 (August 2011): 121–31. <https://doi.org/10.1145/1978542.1978568>.
- Ye, Zhang-Dong, Dong Pan, Zhen Sun, Chun-Guang Du, Liu-Guo Yin, and Gui-Lu Long. 'Generic Security Analysis Framework for Quantum Secure Direct Communication'. *Frontiers of Physics* 16, no. 2 (28 December 2020): 21503. <https://doi.org/10.1007/s11467-020-1025-x>.
- Zambrano, Vittorio. 'Il Nuovo Capitolato AIPA.' *Enti Pubblici*, no. 2 (1997): 149–67.
- Zebrowski, Chris, and Daniel Sage. 'Resilience and Critical Infrastructure: Origins, Theories, and Critiques'. In *The Palgrave Handbook of Security, Risk and Intelligence*, edited by Robert Dover, Huw Dylan, and Michael S. Goodman, 117–35. London: Palgrave Macmillan UK, 2017. [https://doi.org/10.1057/978-1-137-53675-4\\_7](https://doi.org/10.1057/978-1-137-53675-4_7).