DOCUMENTI 19 Giugno 2025

SPUNTI DI RIFLESSIONE SULLA PROPOSTA DI LEGGE IN MATERIA DI SEQUESTRO DI DISPOSITIVI E DI DATI

Jacopo Della Torre

Pubblichiamo di seguito il testo dell'audizione del prof. Jacopo Della Torre dinnanzi alla Commissione Giustizia della Camera dei Deputati nell'ambito dell'esame della proposta di legge C. 1822, approvata dal Senato, recante “Modifiche al Codice di procedura penale in materia di sequestro di dispositivi, sistemi informativi o telematici o memorie digitali" (27 maggio 2025).

Il testo è consultabile anche in allegato.

***

- **La necessità (e l’urgenza) dell’intervento in esame**

Desidero aprire il mio intervento esprimendo **piena condivisione** rispetto allo **spirito di fondo** che anima il progetto di legge in esame. Va detto con chiarezza che un intervento del legislatore in questa materia non è soltanto auspicabile, ma **assolutamente necessario e improcrastinabile**.

Difatti, sebbene l'acquisizione di evidenze digitali rappresenti uno **strumento chiave** nella lotta alla criminalità, l'ordinamento processuale vigente si presenta, sotto questo profilo, carente di una disciplina idonea a garantire un equilibrato bilanciamento tra esigenze investigative e tutela di plurimi diritti fondamentali della persona, riconosciuti dalla Costituzione e dalle Carte internazionali sui diritti umani. Tra questi, in primo piano, il **diritto al rispetto della vita privata**, alla **protezione dei dati personali**, alla **libertà e segretezza delle comunicazioni**. Del resto – come ha affermato il *Chief Justice* John Roberts nella celebre sentenza *Riley v. California***[1]** della Corte Suprema degli Stati Uniti – non va dimenticato che «*modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many* [...] *the privacies of life*». Una riflessione, questa, che ci ricorda come i dispositivi digitali non siano più semplici strumenti di comunicazione, ma, oramai, vere e proprie estensioni dell'**identità personale**, custodi della dimensione più intima dell'individuo, e pertanto meritevoli di una protezione rafforzata da parte dell'ordinamento.

Com'era inevitabile, in assenza di una disciplina legislativa adeguata, è stata fino a oggi **la giurisprudenza** a esercitare una **funzione di supplenza**, certamente significativa e apprezzabile**[2]**. Tuttavia, tale supplenza non può ritenersi sufficiente, né sotto il profilo della certezza interpretativa, né rispetto all'esigenza di uniformità applicativa sul territorio nazionale. Senza contare che essa non è, inevitabilmente, idonea a colmare le tensioni che si determinano rispetto al **principio di legalità processuale**, il quale – come noto – ha rango costituzionale, ai sensi dell'art. 111, comma 1, Cost.

Peraltro, la necessità di un intervento normativo in questa materia si è fatta ancora più urgente a seguito della recente sentenza della **Corte di giustizia dell'Unione europea del 4 ottobre 2024 nella causa C-548/21[3]** (*CG* c. *Bezirkshauptmannschaft Landeck*), la quale ha enunciato alcuni principi che risultano particolarmente critici per l'attuale assetto del sistema penale italiano.

In tale pronuncia, la Corte ha stabilito, in estrema sintesi, che:

A) L'articolo 4, paragrafo 1, lettera c), della direttiva (UE) 2016/680, letto alla luce degli articoli 7, 8 e 52, par. 1, della Carta dei diritti fondamentali dell'Unione europea, **non osta** a una normativa nazionale che consenta alle

autorità competenti di **accedere ai dati contenuti in un telefono cellulare** per finalità di prevenzione, indagine e perseguimento dei reati, **a condizione che**:

- la normativa definisca in modo sufficientemente preciso **la natura o le categorie dei reati in questione**;
- venga rispettato il **principio di proporzionalità**;
- tale accesso sia subordinato, salvo casi di urgenza debitamente giustificati, a un **controllo preventivo da parte di un giudice** o di un'autorità amministrativa indipendente.

B) Gli articoli 13 e 54 della direttiva 2016/680, interpretati alla luce degli articoli 47 e 52, par. 1, della Carta, **ostano** a una normativa nazionale che consenta alle autorità di **tentare di accedere a dati** contenuti in un telefono cellulare **senza informare l'interessato dei motivi sui quali si fonda l'autorizzazione ad accedere a tali dati**, qualora sia **venuto meno il rischio che tale comunicazione comprometta l'efficacia delle indagini**.

Al riguardo, va osservato che, in forza del **principio di primato del diritto dell'Unione europea**, gli effetti di tale pronuncia della Corte di giustizia si riverberano inevitabilmente anche sull'ordinamento interno. Ed è proprio la consapevolezza di ciò che ha portato la Corte di cassazione in una recente sentenza a riconoscere l'inadeguatezza dell'attuale quadro normativo rispetto ai principi di diritto così affermati in sede eurounitaria. In particolare, sconfessando apertamente un proprio precedente, la Suprema Corte ha affermato: «**certamente** […] **allo stato la normativa interna non risponde alla previsione della citata Direttiva** – e dell'interpretazione che deve essere data anche alla norma di attuazione interna di cui all'art. 3 del d.lgs. 18 maggio 2018, n. 51 –, che richiede che il **giudice intervenga in via preventiva** con una pronuncia di carattere autorizzatorio»**[4]**. Ancora, in un'ulteriore pronuncia sul medesimo tema, la Corte ha aggiunto che gli autorevoli rilievi formulati dai giudici europei «**sono primariamente rivolti al legislatore**, in relazione all'operatività delle disposizioni della direttiva di riferimento, essendo fra l'altro configurabili diversi modelli procedurali volti ad attuare le indicazioni contenute nella richiamata sentenza»**[5]**. Si tratta di passaggi di estrema rilevanza che, al di là dell'eventuale questione relativa all'efficacia diretta delle norme richiamate dalla Corte di giustizia**[6]**,

confermano **l'assoluta urgenza di un intervento legislativo**, volto ad assicurare la piena conformità dell'ordinamento nazionale agli *standard* di tutela elaborati in sede europea.

Quanto precede dimostra con chiarezza **la complessità delle sfide** che si trova ad affrontare la presente proposta di legge. Una complessità che non deriva soltanto dalla necessità di disciplinare fenomeni connessi a tecnologie in costante e rapida evoluzione, ma, per l'appunto, anche dal fatto che **il testo approvato dal Senato della p.d.l. c. 1822 è stato concepito in un momento antecedente** alla recente pronuncia della Corte di giustizia, qui richiamata.

Nonostante tale difficoltà di fondo, bisogna riconoscere che **la proposta attualmente in esame presenta alcuni indubbi punti di forza**, che la rendono certamente un passo avanti rispetto allo *status quo*.

Mi limito, in questa sede, a richiamarne tre, tra i più significativi:

a) l'introduzione dell'obbligo di **autorizzazione giudiziale preventiva per il sequestro** di dispositivi, sistemi informatici o telematici, nonché di memorie digitali;

b) la volontà di attribuire rilievo espresso ai principi **di proporzionalità, adeguatezza e stretta necessità** in tema di sequestro e perquisizioni informatiche;

c) il tentativo di risolvere l'annosa questione del sequestro della messaggistica e delle *chat*, in linea con le indicazioni fornite dalla **Corte costituzionale nella sentenza 27 luglio 2023, n. 170[7]**, nonché provenienti dalla **giurisprudenza europea** (sia della Corte europea dei diritti dell'uomo**[8]**, sia della Corte di giustizia**[9]**), attraverso l'attribuzione **al giudice** del potere di autorizzare l'acquisizione dei dati di contenuto comunicativo**[10]**.

Se quanto appena osservato è vero, va rilevato come l'attuale formulazione del testo normativo presenti, comunque, **molteplici profili critici**, su cui pare opportuno concentrare l'attenzione nel prosieguo della presente analisi.

- **I punti critici della proposta: la tecnica normativa nella redazione dell'art. 254-*ter* c.p.p.**

Il primo aspetto su cui è necessario concentrare l'attenzione è di ordine metodologico. La disposizione cardine che il progetto di legge intende introdurre – attorno alla quale ruotano tutte le altre – è rappresentata dall'art. 254-*ter* c.p.p. Orbene, va rilevato come tale articolo risulti di **difficile lettura**, a causa della sua **eccessiva estensione** – articolata in ben 19 commi – che finirebbe per renderlo la disposizione per distacco più lunga dell'intero codice di rito.

A ben vedere, il problema di fondo risiede, da questa prospettiva, nel fatto che, mediante tale disposizione, si è tentato di accorpare in un'unica sede discipline tra loro eterogenee, riconducibili a **istituti distinti**, tanto nei presupposti applicativi, quanto nelle implicazioni procedimentali.

In particolare, si possono individuare almeno sei nuclei tematici principali:

a) la disciplina (ordinaria e accelerata) del sequestro di dispositivi, sistemi informatici o telematici e memorie digitali (commi 1-5), ovvero del "contenitore" di dati;

b) le regole relative alla duplicazione del contenuto dei "contenitori" appresi (commi 6-11);

c) le modalità di selezione e sequestro dei dati pertinenti (commi 12-14);

d) le ipotesi in cui il sequestro si renda necessario dopo l'esercizio dell'azione penale (comma 15);

e) la disciplina della conservazione del duplicato informatico (commi 16-18);

f) i rimedi impugnatori, con particolare riferimento al riesame (comma 19).

Com'è inevitabile, una simile concentrazione normativa – pur animata dall'intento di offrire una struttura organica e unitaria – finisce per dar vita a una **disciplina farraginosa e di difficile applicazione pratica**, risultando, per di più, fonte di ambiguità interpretative e di **aporie sistematiche[11]**.

Proposta emendativa:

Per far fronte a tale criticità, e in coerenza con i **principi di semplicità, chiarezza e precisione enunciati** nelle *Regole e raccomandazioni per la formulazione tecnica dei testi legislativi adottate da Camera e Senato***[12]**,

sarebbe auspicabile procedere a una **scomposizione dell'attuale versione dell'art. 254-*ter* c.p.p.** in una serie di disposizioni distinte e coordinate, ciascuna dedicata a uno specifico profilo. Una simile scelta tecnica favorirebbe una più agevole comprensione del testo e una sua applicazione pratica più ordinata e sistematica.

- **Problematiche in tema di vaglio di proporzionalità in astratto per il sequestro di dispositivi, sistemi informatici o telematici e memorie digitali, nonché per l'apprensione di dati diversi da quelli comunicativi**

Definiti i profili preliminari di ordine metodologico, è ora opportuno soffermarsi sul piano contenutistico.

A questo proposito, occorre innanzitutto concentrare l'attenzione sul fatto che l'attuale formulazione dell'art. **254-*ter*** c.p.p. – diversamente da quanto previsto, ad esempio, per le intercettazioni o per l'acquisizione dei tabulati telefonici e telematici – non contempla alcuna delimitazione, né qualitativa né quantitativa, dei reati per i quali risulti ammissibile:

a) **il sequestro di dispositivi elettronici, sistemi informatici o telematici**;

b) **l'apprensione di dati a contenuto non comunicativo**.

Diversamente, per quanto riguarda l'acquisizione di **dati di matrice comunicativa**, è presente un riferimento espresso all'elenco contenuto nell'art. **266, comma 1, c.p.p**. – richiamato dal comma 12 del medesimo art. 254-*ter* – determinandosi così una selezione fondata sulla gravità dei reati analoga a quella prevista per le intercettazioni.

Ebbene, è opportuno rilevare come tale struttura di fondo risulti **problematica** proprio alla luce di quanto affermato dalla **Corte di giustizia nella già menzionata sentenza del 4 ottobre 2024 (causa C-548/21)**. In tale pronuncia i giudici di Lussemburgo, pur avendo chiarito che il tentativo di accesso a un dispositivo elettronico nell'ambito di un'indagine penale non deve essere necessariamente limitato al perseguimento di forme "gravi" di criminalità, hanno altresì affermato che, in conformità al principio di proporzionalità sancito dall'art. 52, par. 1, della Carta dei diritti fondamentali dell'Unione europea, ogni limitazione all'esercizio di un diritto fondamentale

deve essere "prevista dalla legge". Tale requisito implica, secondo la Corte, la necessaria esistenza di una base giuridica sufficientemente chiara e precisa, capace di definire, già in astratto, con adeguato dettaglio la portata e i limiti dell'ingerenza nei diritti garantiti. Ne consegue che, per soddisfare tale parametro, il legislatore nazionale è tenuto a determinare, per usare le parole della Corte, «**in modo sufficientemente preciso gli elementi, in particolare la natura o le categorie dei reati di cui trattasi, da prendere in considerazione**»**[13]**. Da questa prospettiva, l'assenza, nell'attuale formulazione dell'art. **254-*ter*** c.p.p., di una selezione qualitativa e/o quantitativa delle ipotesi di reato che legittimano il sequestro di dispositivi digitali e di dati diversi da quelli comunicativi solleva rilevanti profili di criticità rispetto agli *standard* europei, in particolare con riguardo al **principio di proporzionalità**.

Proposta emendativa:

Per rimediare a tale criticità, si suggerisce di **selezionare, a monte, in via generale e astratta le categorie di reato che possano giustificare, tanto il ricorso al sequestro di dispositivi, quanto l'accesso a dati digitali non comunicativi**. Sul punto, va, peraltro, precisato che, nell'ottica della giurisprudenza europea, un simile filtro sembra poter essere modellato **in termini meno esigenti** rispetto a quello previsto dagli artt. 266 c.p.p. e 132 del Codice della *privacy*, in quanto l'accesso non deve per forza essere limitato alla criminalità più grave (arg. *ex* § 97 della sentenza della Corte di giustizia *CG*). Una possibilità potrebbe essere fare riferimento ai reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a **due anni**, determinata a norma dell'articolo 4 del codice di procedura penale (più altre fattispecie *ad hoc* selezionate dal legislatore).

Per converso, sul versante dei **dati comunicativi**, il legislatore – al fine di non comprimere eccessivamente i poteri investigativi – potrebbe valutare l'opportunità di ampliare l'elenco delle fattispecie richiamate dall'art. 266 c.p.p., **integrandolo con ulteriori ipotesi non attualmente contemplate[14]**. Una simile scelta potrebbe trovare giustificazione nel fatto che, nell'ambito applicativo dell'art. 254-*ter* c.p.p., l'intrusione nella sfera individuale presenta una connotazione diversa rispetto a quella determinata dalle intercettazioni: essa riguarda, infatti, dati relativi a comunicazioni già

avvenute, e dunque non comporta un'acquisizione contestuale, ma *ex post*, delle informazioni, attenuandosi così – in parte – l'impatto sulla libertà delle comunicazioni.

- **Criticità in tema di vaglio di proporzionalità in concreto**

Sebbene l'attuale formulazione dell'art. 254-*ter* c.p.p. determini, invece, un **esplicito rafforzamento delle garanzie in materia di proporzionalità "in concreto"** – prevedendo una valutazione caso per caso, da parte dell'autorità giudiziaria, circa l'idoneità, la stretta necessità e la proporzionalità in senso stretto del mezzo di ricerca della prova – permangono, anche sotto questo profilo, rilevanti criticità.

Merita menzionarne almeno **quattro**.

A. Il primo profilo critico riguarda l'**assenza di una soglia probatoria minima espressamente prevista** per l'adozione del sequestro di dispositivi, sistemi informatici o telematici, memorie digitali, nonché di dati diversi da quelli comunicativi. La proposta si limita, infatti, a richiamare il canone generale della proporzionalità, senza però individuare uno *standard* probatorio minimo, idoneo a delimitare l'ambito operativo della misura. Si tratta di una lacuna significativa, soprattutto se confrontata con quanto previsto per **altri strumenti di ricerca della prova**: in materia di intercettazioni, l'art. 267, comma 1, c.p.p. richiede la sussistenza di "gravi indizi di reato"; per l'acquisizione dei dati di traffico, l'art. 132, comma 3, del Codice della *privacy* prevede il più lieve *standard* dei "sufficienti indizi di reato". L'assenza di una soglia probatoria di riferimento indebolisce sensibilmente l'effettività del vaglio di proporzionalità in concreto, esponendo la misura al rischio di un uso eccessivamente ampio o meramente esplorativo – fenomeno che la giurisprudenza ha più volte stigmatizzato**[15]**.
B. Il **rischio di sequestri meramente esplorativi** risulta ulteriormente acuito dalla previsione del quarto comma dell'art. 254-*ter* c.p.p., il quale consente, in via ordinaria, la **duplicazione integrale** del contenuto dei dispositivi elettronici, dei sistemi informatici o telematici, nonché delle memorie digitali oggetto di sequestro. Difatti, la disposizione non prevede, al riguardo, **criteri selettivi *ex ante*** volti a circoscrivere l'acquisizione ai soli dati effettivamente pertinenti, con la conseguenza

che il pericolo di apprensioni indiscriminate e totalizzanti di ingenti masse di dati informatici non risulta adeguatamente neutralizzato.

Sennonché, va detto che una simile impostazione si pone in **tensione rispetto all'orientamento consolidato della giurisprudenza di legittimità**, secondo cui «è illegittimo, per violazione del principio di proporzionalità e adeguatezza, il sequestro a fini probatori di un dispositivo elettronico che comporti, **in assenza di specifiche ragioni, l'indiscriminata apprensione di una massa di dati informatici, senza alcuna previa selezione e senza l'indicazione dei criteri eventualmente adottati a tal fine**»**[16]**.

In coerenza con tale principio di diritto, sarebbe stato quanto meno necessario introdurre, già nella fase autorizzativa, un **obbligo di motivazione rafforzata** in capo all'autorità procedente, finalizzato a esplicitare **le ragioni che rendano imprescindibile il ricorso a un sequestro esteso e onnicomprensivo**. Come precisato dalla giurisprudenza, un tale obbligo avrebbe dovuto essere parametrato, in particolare, alla tipologia del reato per cui si procede, al contenuto della condotta contestata, al ruolo attribuito al soggetto titolare dei beni digitali, nonché alla difficoltà di individuare *ex ante* – con precisione – l'oggetto del sequestro**[17]**. Ciò avrebbe consentito di rafforzare il controllo di legalità a monte dell'operazione di duplicazione, e non solo a valle, nella fase di selezione dei dati da parte del pubblico ministero, come previsto dall'attuale versione del comma 12.

C. Con riguardo alla **fase di selezione** dei dati rilevanti, suscita, invece, forti perplessità l'**assenza**, nella disciplina dettata dall'art. 254-*ter*, comma 12, c.p.p., **di un termine entro cui il pubblico ministero o il giudice siano tenuti a procedere alla cernita del materiale informatico duplicato**. A differenza della fase di duplicazione, per la quale è prevista una scansione temporale precisa, il progetto omette, infatti, di imporre un limite temporale all'attività selettiva, lasciandola priva di una cornice cronologica vincolante. Tale lacuna espone al rischio concreto di un'irragionevole protrazione della compressione dei diritti fondamentali della persona, con possibili interferenze prolungate nella sfera privata e informativa dell'individuo, in contrasto con il principio di stretta necessità.

Ancora, sul piano temporale, ulteriori preoccupazioni emergono dal disposto del **comma 17** del medesimo articolo, che consente la conservazione dell'intero duplicato informatico fino alla pronuncia della sentenza irrevocabile. Anche una simile previsione comporta una disponibilità protratta nel tempo dell'integralità dei dati acquisiti, oltre quanto strettamente necessario ai fini dell'accertamento. Né, è bene precisarlo, tale compressione della sfera privata **risulta adeguatamente bilanciata** dalla disposizione che consente agli interessati di richiedere al giudice la distruzione dei dati, delle informazioni e dei programmi contenuti nel duplicato, qualora non risultino necessari per il procedimento. Si tratta, infatti, di una tutela che trasferisce sulle parti un onere significativo – e non sempre agevolmente esercitabile – finendo così per legittimare, a monte, una compressione generalizzata e potenzialmente sproporzionata del diritto alla riservatezza.

In definitiva, va detto che questa impostazione normativa risulta, nel suo complesso, **difficilmente conciliabile con l'orientamento ormai consolidato della Corte di cassazione**, secondo cui «l'estrazione di copia integrale dei dati contenuti in dispositivi informatici o telematici realizza una mera copia-mezzo, che legittima la restituzione del dispositivo, ma **non giustifica il trattenimento della totalità delle informazioni apprese oltre il tempo strettamente necessario alla selezione di quelle pertinenti al reato per cui si procede**». La stessa giurisprudenza ha, inoltre, chiarito che «il pubblico ministero è tenuto a predisporre un'organizzazione adeguata per compiere tale selezione nel **tempo più breve possibile**, specialmente quando i dati siano stati sequestrati a soggetti estranei al reato, e a restituire la copia integrale agli aventi diritto una volta completata la selezione»**[18]**.

Alla luce di tali rilievi, sarebbe stato auspicabile **evitare di consentire il mantenimento indiscriminato della copia-mezzo e, al contempo, prevedere l'introduzione di un termine massimo per la selezione dei dati duplicati**, eventualmente prorogabile con provvedimento motivato dell'autorità procedente in presenza di esigenze di particolare complessità.

D. Un ultimo profilo critico concerne il comma 12 dell'art. 254-*ter* c.p.p., dedicato al sequestro dei dati ricavati dal contenitore oggetto di prima apprensione, nella parte

in cui introduce un **regime differenziato** in base alla tipologia delle informazioni da acquisire. In particolare, se si tratta di dati comunicativi, l'autorizzazione spetta al **giudice**; in tutti gli altri casi, è sufficiente l'intervento del **pubblico ministero**.

Tale differenziazione, a una prima lettura, potrebbe apparire coerente con la già menzionata sentenza della Consulta n. 170 del 2023, che ha attribuito copertura costituzionale – *ex* art. 15 Cost. – esclusivamente a dati comunicativi, quali le conversazioni via *chat* contenute in uno *smartphone*. Da qui, l'opzione legislativa di prevedere una riserva di giurisdizione limitata ai soli dati comunicativi, in analogia con quanto avviene per le intercettazioni (art. 267 c.p.p.) e per l'acquisizione dei tabulati telefonici (art. 132 del Codice della privacy).

Tuttavia, anche sotto questo profilo, emergono rilevanti criticità. Si afferma un tanto dal momento che **numerose categorie di dati che non rientrano nella nozione di "comunicativi"** in senso stretto **possono comunque presentare un elevato potenziale lesivo della sfera privata dell'individuo**. Si pensi, ad esempio, alle immagini archiviate sul dispositivo, ai dati di geolocalizzazione, ai registri di navigazione o alle informazioni biometriche, che, considerate nel loro complesso, possono consentire una ricostruzione puntuale delle abitudini di vita, dei movimenti e delle relazioni personali del soggetto interessato.

Ed è in considerazione di questa elevata capacità intrusiva che la giurisprudenza della **Corte di Giustizia dell'Unione europea** – la quale, è bene ribadirlo, ha concentrato la propria attenzione non tanto sul sequestro del contenitore (disciplinato nel caso della p.d.l. in esame dal comma 1 dell'art. 254-*ter*), quanto sull'accesso ai dati in esso contenuti (cui si riferisce il comma 12 del medesimo art. 254-*ter*) – ha affermato con chiarezza, nella già richiamata sentenza del 4 ottobre 2024, che **qualsiasi forma di accesso a un dispositivo tecnologico deve essere previamente sottoposta al vaglio di un giudice o di un'altra autorità terza e imparziale**. Ciò che rileva, nella prospettiva della Corte di Lussemburgo, non è, infatti, la natura comunicativa o meno dei dati, bensì:

a. il grado di interferenza che l'accesso a tali informazioni è idoneo a determinare sulla sfera privata dell'individuo;

b. il fatto che il soggetto incaricato di autorizzare l'intrusione nella sfera del singolo disponga di tutti i poteri e presenti tutte le garanzie necessarie per assicurare un contemperamento dei vari legittimi interessi e diritti in gioco**[19]**.

Proprio alla luce di tali esplicite affermazioni della Corte, **non sembra possibile ritenere che la struttura del pubblico ministero italiano – pur connotata da una significativa indipendenza – possa ritenersi conforme agli *standard* europei**; e ciò in quanto l'organo dell'accusa, per sua natura, non appare sufficientemente terzo rispetto alle indagini da poter garantire quel bilanciamento tra esigenze investigative e tutela dei diritti fondamentali che i giudici europei individuano come elemento imprescindibile per la legittimità di tali misure intrusive.

Proposte emendative (sintesi):

A. Introdurre uno *standard* di prova (ad es. "sufficienti indizi di reato") per l'adozione del sequestro di dispositivi, sistemi informatici o telematici, memorie digitali, nonché di dati diversi da quelli comunicativi.

B. Introdurre un obbligo di motivazione rafforzata in capo all'autorità procedente, finalizzato a esplicitare le ragioni che rendano imprescindibile il ricorso a un sequestro esteso e onnicomprensivo.

C. Evitare di consentire il mantenimento indiscriminato della copia-mezzo e, al contempo, prevedere l'introduzione di un termine massimo per la selezione dei dati duplicati.

D. Richiedere, in ogni caso, l'autorizzazione al giudice all'accesso ai dati, indipendentemente dalla loro natura comunicativa, laddove gli stessi siano idonei a determinare un'intrusione grave nella sfera giuridica della persona**[20]**.

- **Criticità sul piano del diritto di difesa**

Anche sul piano della salvaguardia dei **diritti della difesa** la proposta di legge, pur determinando un passo avanti rispetto allo *status quo*, presenta vari profili problematici.

A. Il primo profilo critico attiene al tema dell'**informazione all'indagato** circa i motivi su cui si fonda l'autorizzazione ad accedere ai dati appresi attraverso il sequestro. Si tratta di un aspetto particolarmente delicato, in quanto espressamente valorizzato, anche in questo caso, dalla Corte di giustizia dell'Unione europea, la quale ha chiarito che **non è sufficiente che il soggetto interessato sia a conoscenza del sequestro del dispositivo, ma è necessario che venga informato del tentativo di accesso ai dati da parte dell'autorità**, quantomeno a partire dal momento in cui tale comunicazione non rischi più di compromettere le indagini**[21]**.

   Purtroppo, l'attuale formulazione dell'art. 254-*ter* c.p.p. **risulta carente su questo punto**. In particolare, il comma 12 non prevede alcuna forma di informazione preventiva specifica all'indagato in relazione all'accesso ai dati contenuti nel dispositivo. Nel disegno riformatore, la difesa viene a conoscenza di tale attività solo in un momento successivo, tipicamente al momento della notifica dell'avviso di conclusione delle indagini preliminari *ex* art. 415-*bis* c.p.p.; oppure attraverso l'ordinanza applicativa di una misura cautelare (art. 293 c.p.p.); ovvero in sede di giudizio immediato (art. 454 c.p.p.) o di procedimento per decreto (art. 461 c.p.p.).

   In definitiva, una simile impostazione appare problematica rispetto agli *standard* di tutela elaborati dalla Corte di giustizia dell'Unione europea, i quali impongono che l'interessato sia informato dell'accesso tempestivamente non appena ciò sia possibile senza pregiudizio concreto per le indagini. È vero che l'art. 415-*bis* c.p.p. segna il momento formale della conclusione della fase investigativa e rappresenta, nel sistema attuale, lo snodo fisiologico in cui la difesa viene a conoscenza dell'attività svolta dall'accusa. Tuttavia, non pare conforme al parametro eurounitario adottare una valutazione meramente astratta o generalizzata del possibile pregiudizio investigativo. Al contrario, occorre una **valutazione caso per caso**, fondata su elementi concreti e attuali, così da non

procrastinare oltre il necessario la possibilità per l'interessato di esercitare un controllo effettivo e di approntare un'adeguata strategia difensiva.

B. Il secondo profilo problematico – strettamente connesso a quello appena evidenziato – riguarda l'**assenza di ogni forma di partecipazione difensiva nella procedura di analisi del duplicato informatico** e nella successiva **selezione dei dati da sottoporre a sequestro**. Il comma 12 dell'art. 254-*ter* c.p.p. esordisce, infatti, al riguardo con la formula: «effettuata l'analisi del duplicato informatico, il pubblico ministero», chiarendo così che è il pubblico ministero a individuare i dati da sequestrare.

È vero che la norma prevede criteri rigorosi per l'individuazione dei dati rilevanti, richiedendo che essi siano «strettamente pertinenti al reato, in relazione alle circostanze di tempo e di luogo del fatto e alle modalità della condotta, nel rispetto dei criteri di necessità e proporzione». Tuttavia, il nodo critico rimane l'**esclusione della difesa da questa fase selettiva**, che per sua natura incide profondamente sugli equilibri tra potere investigativo e garanzie del contraddittorio. In particolare, non è prevista alcuna possibilità per la difesa di intervenire nella determinazione dei **criteri tecnici e metodologici utilizzati per l'analisi del dato informatico**, nonostante sia ben noto come la scelta del metodo di estrazione e selezione incida significativamente sugli esiti dell'attività investigativa e sull'effettività della tutela difensiva.

Una parziale reintegrazione delle garanzie difensive è prevista, anche in questo caso, solo in un momento successivo, con il nuovo comma 2-*ter* dell'art. 415-*bis* c.p.p., dove si prevede che «l'avviso contiene altresì l'avvertimento che l'indagato e il suo difensore hanno facoltà di esaminare i dati, le informazioni e i programmi oggetto di sequestro ai sensi dell'articolo 254-ter, comma 12, e il diritto alla trasposizione dei dati, delle informazioni o dei programmi medesimi su supporto idoneo». Tuttavia, si tratta di una fase avanzata e unilaterale, che interviene a valle della selezione dei dati, quando l'interferenza si è già realizzata**[22]**.

Una soluzione più equilibrata sarebbe stata quella di prevedere, come regola generale, un'**udienza preventiva di stralcio** – analoga a quella disciplinata dall'art. 268 c.p.p. in materia di intercettazioni – da svolgersi dinanzi al giudice, con la partecipazione delle parti, al fine di verificare la rilevanza dei dati da acquisire e definire in modo condiviso i criteri di selezione. Soltanto in presenza di **motivate esigenze investigative** – ad esempio pericolo di inquinamento probatorio o urgenza – si sarebbe potuta ammettere, in via eccezionale, una disciplina fondata sul solo successivo accesso difensivo in sede di avviso di conclusione dele indagini *ex* art. 415-*bis* c.p.p.

C. Va rilevato, infine, che la disciplina in esame risulta priva di un adeguato coordinamento con le norme sulle **investigazioni difensive** (artt. 391-*bis* ss. c.p.p.), nell'ambito delle quali può sorgere l'esigenza, da parte del difensore, di acquisire dati digitali secondo modalità rituali, al fine di poterli utilmente spendere nell'interesse dell'assistito – siano essi l'indagato, la persona offesa, o persino un ente potenzialmente destinatario di un'imputazione *ex* d.lgs. 8 giugno 2001, n. 231.

È vero che, anche da questa prospettiva, l'intervento del nuovo art. 415-*bis*, comma 2-*ter*, c.p.p. assume un certo rilievo, prevedendo che «il difensore può, entro il termine di venti giorni, esaminare il duplicato e depositare richiesta motivata di sequestro dei dati, delle informazioni e dei programmi specificamente indicati come rilevanti in relazione alle circostanze di tempo e di luogo del fatto e alle modalità della condotta, nel rispetto dei criteri di necessità e proporzione». Tuttavia, questa facoltà difensiva interviene **solo con riferimento a dati e strumenti già acquisiti su iniziativa dell'autorità procedente**, non configurando un canale autonomo attraverso cui la difesa possa ottenere, in piena parità, l'accesso a fonti digitali d'interesse. In una materia altamente tecnica e delicata come quella dell'acquisizione di dati digitali, dove l'osservanza del principio di legalità è spesso interpretata in termini particolarmente stringenti, sarebbe stato auspicabile un aggiornamento della disciplina delle indagini difensive, tale da consentire anche alla difesa l'attivazione di procedure di acquisizione digitale regolate e garantite. Diversamente, si rischia di

determinare frizioni con il principio di parità delle armi, sancito tanto dall'art. 111 della Costituzione quanto dall'art. 6 della Convenzione europea dei diritti dell'uomo.

Proposte emendative (sintesi):

A. Modificare il comma 12, onde contemplare un meccanismo informativo sul tentativo di accesso ai dati, in coerenza con la giurisprudenza della Corte di Giustizia.

B. Modificare il comma 12, al fine di prevedere, in linea di principio, una forma di contraddittorio anticipato sulla selezione dei dati rilevanti.

C. Introdurre una nuova previsione nelle investigazioni difensive (ad es. dopo l'art. 391-*septies* c.p.p.), in tema di richiesta di sequestro da parte della difesa di contenitori di dati o direttamente di informazioni digitali necessarie per esercizio dei diritti del soggetto rappresentato.

- **Le lacune in tema di "sanzioni processuali"**

Un ulteriore profilo particolarmente delicato riguarda il **piano dei rimedi processuali**. Si tratta di un aspetto cruciale, poiché – come sempre accade – la reale effettività di una disciplina dipende dalla disponibilità di strumenti reattivi che consentano ai soggetti del procedimento di far valere, in concreto, eventuali violazioni delle previsioni normative.

Da questa prospettiva, il disegno normativo fa affidamento principalmente su due strumenti: da un lato, l'istituto della **revoca** del sequestro del contenitore, disciplinato dal comma 3 dell'art. 254-*ter* c.p.p.; dall'altro, la facoltà di proporre **riesame** avverso tutti i provvedimenti di sequestro, sia quelli relativi al contenitore sia quelli riguardanti il contenuto, garantita dal comma 19.

Tuttavia, ciò che **manca** nella disciplina *in fieri* è una **previsione esplicita in materia di inutilizzabilità** delle risultanze ottenute in violazione delle disposizioni di legge. L'unico riferimento in tal senso è contenuto in una

clausola di rinvio all'art. 271 c.p.p., "in quanto compatibile", disposizione che prevede l'inutilizzabilità dei risultati delle intercettazioni se eseguite fuori dei casi consentiti dalla legge o in violazione delle disposizioni previste dagli artt. 267 e 268, commi 1 e 3.

Questo rinvio, peraltro, si presta a **interpretazioni potenzialmente divergenti**. Secondo una possibile lettura restrittiva, si potrebbe sostenere che la clausola di compatibilità rinvii all'art. 271 c.p.p. solo per quanto concerne i dati comunicativi, escludendo così l'inutilizzabilità per tutte le altre categorie di dati digitali acquisiti, pur se in violazione delle garanzie previste. Al contrario, secondo un'interpretazione estensiva, si potrebbe ritenere che l'intera disciplina contenuta nell'art. 254-*ter* c.p.p. goda di una tutela analoga a quella delle intercettazioni, proprio in virtù di una analogia funzionale con la disciplina di tale mezzo di ricerca della prova: in entrambi i casi, infatti, si è in presenza di strumenti investigativi ad elevato potenziale intrusivo, che incidono su diritti fondamentali della persona, e per i quali l'effettività delle garanzie procedurali non può prescindere dalla previsione di una sanzione processuale forte, quale appunto l'inutilizzabilità.

Sennonché, il rischio, in assenza di un'indicazione normativa chiara, è quello di determinare un **quadro giurisprudenziale disomogeneo e instabile**, con conseguenti ricadute sulla certezza del diritto. In particolare, l'eventuale affermazione di orientamenti tesi a escludere l'inutilizzabilità per vizi formali o sostanziali nella procedura di sequestro potrebbe pregiudicare gravemente l'effettività della tutela, svuotando di significato le garanzie previste dal legislatore. In tal caso, infatti, l'ordinamento si affiderebbe unicamente al giudizio *ex post* di attendibilità del dato, rimettendo al soggetto interessato l'onere di dimostrare l'irregolarità dell'acquisizione, e al giudice il compito di valutarne le ricadute probatorie, con il rischio concreto che la disciplina si riveli meramente teorica e illusoria, anziché effettiva e concretamente azionabile.

Proposta emendativa:

Tutto ciò porta a dire che sarebbe preferibile **introdurre una previsione autonoma e specifica di inutilizzabilità**, che sancisca, in modo esplicito, l'invalidità dei dati ottenuti in violazione dell'art. 254-*ter* c.p.p.**[23]**, così da

rafforzare il carattere effettivo e vincolante delle garanzie previste dalla nuova disciplina.

- **Le lacune in tema di disposizioni transitorie**

Un ultimo profilo di rilievo, meritevole di intervento migliorativo, riguarda **l'art. 4 della proposta di legge**, dedicato alla **disciplina transitoria**. Tale disposizione si limita, attualmente, a stabilire che: «le disposizioni di cui alla presente legge si applicano alle perquisizioni e ai sequestri la cui esecuzione ha avuto inizio in data successiva a quella della sua entrata in vigore». Ebbene, va, al riguardo, osservato come si tratti di una previsione ispirata al principio generale del *tempus regit actum*, che, tuttavia, non offre una risposta adeguata ai problemi applicativi che potrebbero emergere nella prassi, in particolare con riferimento alla possibilità di estendere anche ai procedimenti pendenti i principi espressi dalla Corte di giustizia dell'Unione europea nella sentenza CG del 4 ottobre 2024.

A tale riguardo, è **istruttivo richiamare quanto accaduto in materia di tabulati telefonici**. La mancanza di una disposizione transitoria espressa nel decreto-legge 30 settembre 2021, n. 132, che ha inteso recepire nell'ordinamento interno i principi sanciti nella già menzionata sentenza *HK* della Corte di giustizia (C-746/18), ha dato luogo a un acceso dibattito tra gli operatori circa la retroattività dell'applicazione di tali principi, determinando una situazione di incertezza normativa e applicativa**[24]**. I problemi furono tali da costringere il legislatore, in sede di conversione, a introdurre, con la legge n. 178/2021, il comma 1-*bis* all'art. 1 del decreto, che così stabiliva: «i dati relativi al traffico telefonico, al traffico telematico e alle chiamate senza risposta, acquisiti nei procedimenti penali in data precedente alla data di entrata in vigore del presente decreto, possono essere utilizzati a carico dell'imputato solo unitamente ad altri elementi di prova ed esclusivamente per l'accertamento dei reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni».

Proposta emendativa:

Per evitare il riprodursi di una situazione analoga anche in questo ambito, sarebbe opportuno prevedere sin da ora una **disciplina transitoria più completa**. Essa dovrebbe mirare a un ragionevole bilanciamento tra l'esigenza di garantire il rispetto dei diritti fondamentali e quella di non disperdere le acquisizioni investigative già effettuate, subordinandone però l'utilizzabilità a precisi limiti.

In particolare, si potrebbe prevedere, in modo simile a quanto fatto per i tabulati telefonici, che:

a. i dati digitali acquisiti nei procedimenti anteriori all'entrata in vigore della nuova disciplina possano essere utilizzati soltanto per l'accertamento di reati di particolare gravità, secondo un criterio di selezione analogo a quello già adottato per i tabulati;
b. tale utilizzabilità sia subordinata alla presenza di "altri elementi di prova", così da compensare l'assenza di un provvedimento autorizzativo conforme ai nuovi *standard* procedurali e garantistici.

In questo modo si otterrebbe un bilanciamento più equilibrato tra legalità, effettività della tutela dei diritti e funzionalità dell'azione penale, riducendo sensibilmente il rischio di contrasti giurisprudenziali e di successivi interventi correttivi *ex post*.

- **Conclusioni**

A valle delle considerazioni fin qui svolte – che potrebbero essere ulteriormente sviluppate, in particolare con riferimento alla disciplina delle **ispezioni e delle perquisizioni informatiche [25]** – è possibile avanzare alcune **riflessioni conclusive**.

La prima considerazione è di ordine operativo. Alla luce delle numerose criticità che caratterizzano la proposta di legge **C. 1822**, in relazione ai principi fondamentali sanciti dalla Costituzione e dal diritto dell'Unione europea, essa richiederebbe un intervento emendativo di ampia portata, tale da imporre un **nuovo passaggio al Senato**. Ciò comporterebbe un allungamento non trascurabile dei tempi, fatto particolarmente critico se si

considera la delicatezza della situazione determinata dalla recente sentenza della Corte di giustizia più volte menzionata **del 4 ottobre 2024 nella causa C-548/21**.

In questa prospettiva, **una soluzione possibile** – potenzialmente più rapida – potrebbe consistere nell'utilizzare il materiale acquisito durante i lavori parlamentari (comprese le audizioni e gli emendamenti presentati) per elaborare un nuovo testo, che il Governo potrebbe assumere come base per l'adozione di un **decreto-legge**. Del resto, come già evidenziato, proprio la recente sentenza della Corte di giustizia rappresenta un *novum* tale da conferire **particolare urgenza** a un intervento normativo. Né, è bene precisarlo, si tratterebbe di una prassi inedita: anche in seguito alla sentenza *HK* della Corte di giustizia (C-746/18), si fece ricorso alla decretazione d'urgenza per garantire una risposta tempestiva e adeguata**[26]**. Nel caso in esame, le condizioni appaiono del tutto analoghe, e il progetto attualmente all'esame della Camera potrebbe utilmente fungere da base tecnica e politica per un intervento governativo, da perfezionare, ove necessario, ulteriormente dal Parlamento **in sede di conversione** dell'atto.

La seconda riflessione è di ordine sistemico. Nonostante le criticità evidenziate, la proposta in esame reca con sé un messaggio metodologico chiaro e apprezzabile: quello di voler finalmente intervenire su ambiti di fondamentale rilievo, da tempo trascurati dal legislatore, nonostante i ripetuti allarmi lanciati dalla dottrina e le pressanti sollecitazioni della giurisprudenza, nazionale e sovranazionale. Tuttavia, ciò non basta. Il nostro ordinamento sconta un ritardo strutturale anche rispetto **ad altri settori cruciali**, tuttora privi di un'adeguata cornice normativa. Si pensi, solo per fare alcuni esempi, alle videoriprese, anche con riconoscimento facciale; al tracciamento mediante GPS; all'impiego di sistemi di intelligenza artificiale a fini investigativi e probatori; ai sequestri di cripto-attività; all'utilizzo dell'OSINT (*Open Source Intelligence*); fino all'installazione di *trojan virus* in modalità diverse da quella dell'intercettazione. Si tratta, com'è evidente, di lacune profonde e sistemiche, tanto più gravi se si considera che **oggi la "prova regina" non è più quella dichiarativa, ma quella tecnologica**. È un mutamento strutturale che mette in crisi l'impianto del codice del 1988,

ormai sempre meno adeguato a regolare scenari probatori radicalmente trasformati. Quella che abbiamo di fronte è, insomma, una vera e propria **emergenza normativa**.

Urge, pertanto, un cambio di passo deciso, che consenta di affrontare in modo organico e coerente l'insieme delle problematiche connesse all'acquisizione e alla valutazione della prova digitale nel processo penale. In questa prospettiva, la dottrina ha il compito di richiamare l'attenzione su modelli virtuosi già esistenti. Particolarmente significativa è, in tal senso, l'**esperienza spagnola.** Con la *Ley Orgánica* 13/2015, del 5 di ottobre, il legislatore iberico ha riformato in profondità la *Ley de Enjuiciamiento Criminal*, con l'obiettivo dichiarato di disciplinare in modo sistematico *le medidas de investigación tecnológica*, rafforzando al contempo le garanzie processuali delle persone coinvolte. Degna di nota è, in particolare, l'introduzione di un nucleo di principi generali (*especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad*), destinati a orientare l'uso di qualsiasi strumento di ricerca della prova digitale, secondo una logica di rigore metodologico e di tutela multilivello**[27]**.

L'auspicio è che anche l'Italia possa intraprendere un percorso riformatore altrettanto strutturato e lungimirante, capace di coniugare l'efficienza dell'accertamento penale con la piena salvaguardia dei diritti fondamentali della persona. E la speranza è che la proposta di legge oggi all'esame possa costituire un primo passo in questa direzione.

Genova, 27/5/2025

[1] Cfr. *Riley v. California*, 573 U.S. 373.

[2] Cfr., tra le molte, Cass., sez. II, 13 maggio 2025, n. 18108; Cass., sez. III, 11 febbraio 2025, n. 5526; Cass., sez. IV, 5 giugno 2024, n. 22595; Cass., sez. VI, 15 febbraio 2024, n. 17312; Cass., sez. VI, 3 gennaio 2024, n. 222; Cass.,

sez. VI, 11 gennaio 2022, n. 12507; Cass., sez. VI, 14 giugno 2022, n. 35652; Cass., sez. VI, 19 febbraio 2021, n. 6623; Cass., sez. VI, 22 settembre 2020, n. 34265.

[3] Il riferimento va a Corte giust., 4 ottobre 2024, *Bezirkshauptmannschaft Landeck (Tentative d'accès aux données personnelles stockées sur un téléphone portable)*, Causa C-548/21.

[4] La citazione è tratta da Cass., sez. VI, 8 aprile 2025, n. 13585.

[5] Cfr. Cass., sez. VI, 18 aprile 2025, n. 15500.

[6] Al riguardo, sembra doversi precisare che la strada del riconoscimento di effetti diretti alle norme analizzate dalla Corte di giustizia nella sentenza del 4 ottobre 2024 non appare facilmente percorribile sul piano esegetico, in quanto esse, lasciando spazio a diverse modalità di attuazione da parte degli Stati membri, sembrano mancare dei requisiti di chiarezza, precisione e natura incondizionata richiesti dalla giurisprudenza della Corte a tale scopo. Il che, peraltro, non esclude che debba comunque essere perseguita – nei limiti del possibile – la via dell'interpretazione conforme al diritto dell'Unione. Ciò potrebbe avvenire, ad esempio, attraverso una lettura restrittiva del termine "autorità giudiziaria", presente in diverse disposizioni del codice d rito, tale da attribuire al solo giudice – e non anche al pubblico ministero – il potere autorizzativo in materia di accesso ai dati. In tal senso sembra orientarsi anche la sentenza della Corte di cassazione, sez. VI, 8 aprile 2025, n. 13585.

[7] Come noto, in tale sentenza il Giudice delle Leggi, pur pronunciandosi nell'ambito di un conflitto di attribuzione tra poteri dello Stato, ha chiarito che lo scambio di messaggi elettronici - *e-mail*, SMS, *WhatsApp* e simili - rappresenta, di per sé, una forma di corrispondenza, e ciò anche nel caso in cui si tratti di messaggi già ricevuti e letti dal destinatario, con l'unica eccezione che, in ragione del tempo trascorso, il messaggio non abbia perso ogni carattere di attualità, in rapporto all'interesse alla sua riservatezza, trasformandosi in un mero documento "storico". Tale attualizzazione della nozione di corrispondenza rispetto ai nuovi mezzi di comunicazione ha comportato l'estensione anche ai messaggi elettronici della sfera di tutela prevista dall'art. 15 Cost., che assicura a tutti i consociati la libertà e la

segretezza della corrispondenza e di ogni altra forma di comunicazione, consentendone la limitazione soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge.

[8] Il rinvio va, tra le molte, a Corte EDU, Grande Camera, 25 maggio 2021, *Big Brother Watch e Altri c. Regno Unito*; Corte EDU, sez. I, 17 dicembre 2020, *Saber c. Norvegia*; Corte EDU, Grande Camera, 5 settembre 2017, *Bărbulescu c. Romania;* Corte EDU, sez. IV, 3 aprile 2007, *Copland c. Regno Unito*.

[9] Cfr., tra le molte pronunce sul punto, oltre a quella citata alla nota 3, Corte Giust., 30 aprile 2024, *Ignoti c. Procura della Repubblica presso il Tribunale di Bolzano*, C-178/22; Corte Giust., 30 aprile 2024, L*a Quadrature du Net*, C-470/21; Corte Giust., 7 settembre 2023, *Lietuvos Respublikos generalinė prokuratūra*, C-162/22; Corte Giust., 17 novembre 2022, *Spetsializirana prokuratura*, C-432/22; Corte Giust, 20 settembre 2022, *VD e SR*, C-339/20 e C-397/20; Corte Giust., 20 settembre 2022, *Space Net*, C-793 e 794/19; Corte Giust., 5 aprile 2022, *Commissioner of An Garda Síochána e. a.*, C-140/20; Corte Giust., 2 marzo 2021, *H.K. c. Prokuratuur*, C-746/18; Corte Giust., 6 ottobre 2020, *Privacy International*, C-623/17; Corte Giust, 6 ottobre 2020, *La Quadrature du Net*, C-511/18, C-512/18 e C-520/18; Corte Giust., 2 aprile 2018, *Ministerio Fiscal*, C-207/16; Corte Giust., 21 dicembre 2016, *Tele 2 e Watson*, C-203/15 e C-698/15; Corte Giust., 8 aprile 2014, *Digital Rights Ireland*, C-293/12 e C-594/12. Come noto, il punto focale di questa giurisprudenza consiste nel rilievo per cui le ingerenze gravi negli artt. 7 e 8 della Carta di Nizza, per essere proporzionate ai sensi dell'art. 52 della medesima Carta, devono essere autorizzate da un giudice o da un'autorità amministrativa indipendente, che deve essere in grado di garantire un giusto equilibrio tra i legittimi interessi in gioco. A questo riguardo, la Corte di Lussemburgo ha, del pari, chiarito che la gravità dell'ingerenza nei diritti fondamentali dipende da quanto precise siano le conclusioni rispetto alla vita privata della persona interessata che l'accesso ai dati può determinare.

[10] È utile ricordare come si tratti di una soluzione più garantista rispetto a quella oggi propugnata dalla giurisprudenza di legittimità interna, che ritiene, invece, sufficiente, per quanto concerne il sequestro della messaggistica, la sola iniziativa del pubblico ministero: cfr., *ex multis*, Cass., sez. VI, 28 ottobre 2024, n. 39548; Cass., sez. II, 15 maggio 2024, n. 25549; Cass., sez. un., 29 febbraio 2024, n. 23755 e 23756.

[11] Un esempio emblematico è offerto dall'*incipit* del comma 6, che stabilisce un termine di cinque giorni dal deposito del verbale di sequestro entro il quale il pubblico ministero è tenuto ad avvisare determinati soggetti dell'avvio della procedura di duplicazione. Tale previsione risulta problematica nei casi in cui il sequestro sia stato disposto d'urgenza dal pubblico ministero o dalla polizia giudiziaria, poiché il comma 5 attribuisce al giudice un termine di dieci giorni per la relativa convalida. Sorge, a questo punto, un interrogativo: il termine di cinque giorni previsto dal comma 6 trova applicazione anche in presenza di un sequestro ancora *sub iudice*, perché in attesa di convalida? Una lettura meramente letterale sembrerebbe suggerire una risposta affermativa. Tuttavia, dal punto di vista sistematico e logico, appare poco coerente avviare la procedura di duplicazione prima che il sequestro sia stato confermato dal giudice, e dunque prima che sia accertata la legittimità stessa dell'apprensione.

[12] Cfr. Regole e raccomandazioni per la formulazione tecnica dei testi legislativi, Circolare del Presidente del Senato, 20 aprile 2001, in *www.senato.it*, ove si legge: «ogni precetto normativo contenuto nell'atto è formulato evitando qualsiasi ambiguità semantica e sintattica e rispettando, per quanto possibile, sia il principio della semplicità che quello della precisione» (par. 2, lett. b).

[13] Corte giust., 4 ottobre 2024, *Bezirkshauptmannschaft Landeck (Tentative d'accès aux données personnelles stockées sur un téléphone portable)*, Causa C-548/21, § 99.

[14] Si pensi, ad esempio, alla frode informatica semplice, di cui all'art. 640-*ter,* comma 1, c.p.p.

[15] V., per tutte, Cass., sez. VI, 22 settembre 2020, n. 34265.

[16] Cfr., da ultimo, Cass., sez. II, 13 maggio 2025, n. 18108.

[17] In questo senso, v. Cass., sez. VI, 14 giugno 2022, n. 35652, ove si è chiarito che «in tema di sequestro probatorio, l'acquisizione indiscriminata di un'intera categorie di beni, nell'ambito della quale procedere successivamente alla selezione delle singole *res* strumentali all'accertamento del reato, è consentita a condizione che il sequestro non assuma una valenza meramente esplorativa e che il pubblico ministero adotti una motivazione che espliciti le ragioni per cui è necessario disporre un sequestro esteso e

onnicomprensivo, in ragione del tipo di reato per cui si procede, della condotta e del ruolo attribuiti alla persona titolare dei beni, e della difficoltà di individuare *ex ante* l'oggetto del sequestro».

[18] V., ancora, Cass., sez. II, 13 maggio 2025, n. 18108, da cui è tratta anche la citazione testuale precedente.

[19] Corte giust., 4 ottobre 2024, *Bezirkshauptmannschaft Landeck (Tentative d'accès aux données personnelles stockées sur un téléphone portable)*, Causa C-548/21, § 103, ove si afferma, più precisamente, che «per quanto riguarda più in particolare un'indagine penale, un controllo di questo tipo esige che tale giudice o tale organo sia in grado di garantire un giusto equilibrio tra, da un lato, i legittimi interessi connessi alle necessità dell'indagine nell'ambito della lotta alla criminalità e, dall'altro, i diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali delle persone i cui dati sono interessati dall'accesso».

[20] In particolare, laddove si optasse per una tale soluzione sarebbe opportuno intervenire diversamente, in modo sistemico, anche sulla disciplina delle perquisizioni (e ispezioni) informatiche, richiedendo l'autorizzazione per le stesse al giudice.

[21] Emblematica, al riguardo, è la già citata sentenza Corte giust., 4 ottobre 2024, *Bezirkshauptmannschaft Landeck (Tentative d'accès aux données personnelles stockées sur un téléphone portable)*, Causa C-548/21, § 122, ove si è affermato: «nel caso di specie, dalla decisione di rinvio risulta che CG sapeva che il suo telefono cellulare era stato sequestrato quando le autorità di polizia austriache hanno tentato invano di sbloccarlo al fine di accedere ai dati in esso contenuti. In tali circostanze, non sembra che informare CG del fatto che tali autorità avrebbero cercato di accedere a tali dati rischiasse di compromettere le indagini, cosicché egli avrebbe dovuto esserne preventivamente informato».

[22] È a ogni modo opportuno rilevare, sul punto, che il comma 2-*ter* dell'art. 415-*bis*, di cui si propone l'introduzione, dovrebbe essere rafforzato, prevedendo un ampliamento dei termini concessi alla difesa per l'analisi dei dati, attualmente troppo ristretti nella formulazione proposta.

[23] Ovviamente, un discorso analogo potrebbe essere fatto anche per le altre previsioni "collaterali" contenute nel progetto di legge in esame.

[24] Cfr., ad es., Cass., sez. III, 1° aprile 2022, n. 11991; Cass., sez. V, 6 ottobre 2021, n. 1054.

[25] Ci si riferisce, in prima battuta, al fatto che le disposizioni in materia di ispezioni informatiche (art. 244, comma 2, c.p.p.) ad oggi, non risultano oggetto di un aggiornamento sistematico da parte della novella in esame. A ciò si aggiunge un ulteriore profilo critico, relativo alla disciplina delle perquisizioni informatiche, che – nella formulazione attuale della proposta – continuano a poter essere disposte dal pubblico ministero, e in taluni casi dalla polizia giudiziaria, mediante decreto motivato. Sennonché, il problema è che in tali ipotesi la duplicazione del dispositivo digitale – operazione logicamente e tecnicamente necessaria per poter effettuare una perquisizione – avviene al di fuori di qualsiasi controllo giudiziale preventivo, in evidente antinomia rispetto a quanto previsto dal primo comma dell'art. 254-*ter* c.p.p. Di fatto, dunque, la disciplina in materia di perquisizioni informatiche rischia di vanificare, almeno in parte, le garanzie introdotte proprio con l'art. 254-*ter*, consentendo una forma surrettizia di duplicazione e analisi dei dati digitali priva di autorizzazione giudiziaria. Per evitare tale effetto elusivo, sarebbe necessario prevedere espressamente che, salvo casi d'urgenza, anche le ispezioni e le perquisizioni aventi a oggetto dispositivi o ambienti digitali debbano essere autorizzate dal giudice, secondo un modello uniforme e coerente con le più recenti esigenze di tutela della riservatezza.

[26] Il rinvio va al già menzionato decreto-legge 30 settembre 2021, n. 132, convertito in l.23 novembre 2021, n. 178.

[27] Per una panoramica sui contenuti di tale legge, si vedano: F. Bueno de Mata, *Las diligencias de investigación penal en la cuarta revolución industrial. Principios teóricos y problemas prácticos*, Cizur Menor, 2019; e S. Pereira Puigvert, *Las medidas de investigación tecnológicas y su injerencia en la privacidad de las personas y la protección de datos personales*, in *Investigación y prueba en los procesos penales de España e Italia*, a cura di I. Villar Fuentes, Cizur Menor, 2019, pp. 297 ss.