ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA | DIPARTIMENTO
DI SCIENZE GIURIDICHE

PROF. MICHELE CAIANIELLO
Ordinario di Diritto processuale penale nell'Università di Bologna

CAMERA DEI DEPUTATI — COMMISSIONE II (Giustizia)

MARTEDÌ 27 MAGGIO 2025 - Audizione informale, 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 informatici o telematici o memorie digitali" (disegno di legge C. 806)

Signor Presidente, Onorevoli,

permettetemi in primo luogo di ringraziarvi per l'invito: sono onorato di poter contribuire ai lavori di approfondimento della Commissione Giustizia sulla proposta di legge C. 1822 (Disegno di legge C. 1866), dedicato all'introduzione di alcune modifiche al codice di procedura penale quando occorra condurre operazioni in materia di sequestro di dispositivi, sistemi informatici o telematici o memorie digitali.

La mia analisi si concentrerà prima sul quadro generale della riforma, per poi effettuare alcune osservazioni su specifici passaggi normativi del disegno di legge.

I. Necessità del controllo giurisdizionale nella raccolta e nel trattamento dei dati

1. Finalità dell'intervento normativo

La proposta in esame si colloca nell'alveo di un più ampio processo di aggiornamento del diritto processuale penale, volto a garantire l'effettività dell'azione investigativa senza sacrificare le garanzie fondamentali del soggetto sottoposto ad indagine. In particolare, l'intervento si propone di colmare le lacune interpretative e applicative che l'attuale formulazione degli articoli 253 e seguenti del codice di procedura penale presenta in relazione al sequestro di dispositivi elettronici, server, archivi digitali e contenuti in cloud.

Tali strumenti, oggi sempre più frequentemente utilizzati per la comunicazione, la conservazione di informazioni e l'esercizio di attività personali o professionali, rappresentano contenitori di dati sensibili, molto spesso sovrabbondanti rispetto alle finalità dell'accertamento penale: ciò è dovuto al fatto, ben noto, per cui attraverso la raccolta dei dati contenuti in un dispositivo digitale si ottiene una fotografia estremamente accurata dell'individuo coinvolto (e anche di soggetti terzi), in molteplici ambiti della vita personale (salute, orientamenti politici, preferenze sessuali, condizioni economiche e così via). Di qui, la necessità di una disciplina che rafforzi i presidi di legalità e proporzionalità, come in qualche maniera già anticipato dalla giurisprudenza della Corte Suprema statunitense, che, già dal 2014 sancì la necessità di un *judicial warrant* perché la polizia, in caso di arresto in flagranza, potesse accedere allo smartphone della persona arrestata (Caso *Riley v. California*, 2014).

Idealmente, è evidente il legame tra la riforma in corso e il decreto-legge 30 settembre 2021, n. 132, conv. in l. 23 novembre 2021, n. 178, con il quale è stato modificato l'art. 132 del codice della privacy, per venire incontro ad alcune indicazioni estrapolabili dalla giurisprudenza della Corte europea dei diritti dell'uomo e, soprattutto, della Corte di giustizia dell'Unione europea.

2. L'introduzione del controllo giudiziale nel sequestro di dispositivi digitali

Una delle innovazioni più rilevanti recate dalla proposta di legge in esame consiste nell'introduzione del necessario intervento del giudice per le indagini preliminari (g.i.p.), quale soggetto titolare del potere autorizzatorio o convalidante nei casi in cui si renda necessario procedere al sequestro di dispositivi informatici, sistemi telematici o memorie digitali.

Si tratta di una modifica di significativo rilievo, che segna una discontinuità rispetto all'assetto previgente, in cui tali operazioni erano riconducibili esclusivamente alla sfera di competenza del pubblico ministero. L'inserimento di un vaglio giudiziale rappresenta una risposta coerente e necessaria alle peculiarità che connotano la materia digitale, nella quale il sequestro di un dispositivo non comporta soltanto l'apprensione materiale di un oggetto, ma permette la acquisizione di vasti insiemi di dati (*bulk data*), in buona parte non pertinenti all'indagine, e comunque suscettibili di interferire in misura rilevante con diritti fondamentali della persona (il diritto alla vita privata e familiare, al dominio sui propri dati, alla privacy). La scelta legislativa si impone, pertanto, come positiva e doverosa.

È positiva perché rafforza il sistema delle garanzie processuali, assicurando un più elevato grado di tutela tanto per la persona sottoposta ad indagini quanto per la persona offesa dal reato.

È al contempo doverosa, in quanto espressamente sollecitata dalla giurisprudenza sovranazionale. Numerose sentenze della Corte europea dei diritti dell'uomo - tra le quali si possono menzionare *Zakharov v. Russia*, 4 dicembre 2015, *ric. n.* 47143/06 e *Big Brother Watch and Others V. The United Kingdom*, 25 maggio 2021, ric. nn. 58170/13, 62322/14 and 24960/15 - hanno posto in evidenza l'esigenza di un controllo giurisdizionale effettivo sulle operazioni che implichino ingerenze nella vita privata e nella corrispondenza. Analogo orientamento è riscontrabile nella giurisprudenza della Corte di giustizia dell'Unione europea, che ha più volte ribadito la necessità di un vaglio preventivo, indipendente e imparziale, per garantire il rispetto dei principi di legalità e proporzionalità (*Digital Rights Ireland*, *Tele2 Sverige*, *La Quadrature du Net*, *Prokuratuur*, *Landek*) e altri cui si rinvia nella bibliografia finale).

3. Il contesto delle indagini guidate dai dati (*data-driven investigations*)

L'intervento legislativo si inserisce inoltre in un contesto investigativo profondamente trasformato dall'evoluzione tecnologica. Nell'attuale paradigma operativo, si assiste con crescente frequenza all'impiego di metodologie investigative fondate sull'analisi massiva di dati digitali — prassi che, nel lessico della dottrina e della comparazione giuridica, vengono ormai comunemente identificate come *data-driven investigations*. Si tratta di una trasformazione che ha interessato, in misura variabile, numerose giurisdizioni nazionali, con un progressivo slittamento dell'asse dell'indagine dalla raccolta mirata di prove a posteriori verso un'acquisizione preventiva, generalizzata e strutturata dei dati disponibili.

Dal punto di vista empirico, queste operazioni si articolano in due fasi: una prima fase di captazione e conservazione integrale di una massa di dati grezzi, custoditi in memorie digitali, seguita da una fase di analisi selettiva e retrospettiva finalizzata all'individuazione di elementi probatori rilevanti.

Questo approccio, pur efficace sul piano operativo, solleva interrogativi sul piano delle garanzie costituzionali, richiedendo, a livello codicistico, controlli rafforzati, soprattutto *ex ante*, da parte di un giudice terzo, per evitare che l'indagine si trasformi in una mera esplorazione di dati privi di nesso con la notizia di reato.

4. Il diritto al contraddittorio e le garanzie della difesa

Nel contesto delle investigazioni digitali, assume rilievo essenziale il diritto della difesa a partecipare in modo pieno ed effettivo alle fasi di acquisizione e analisi della prova. Non è sufficiente garantire l'accesso formale ai dati, ma è necessario assicurare le condizioni

per un contraddittorio effettivo, che consenta alla difesa di interloquire criticamente sulle attività svolte dal pubblico ministero e dalla polizia giudiziaria.

La proposta di legge si muove in questa direzione, promuovendo un modello processuale in cui la difesa possa esercitare un controllo tecnico tempestivo, accedere a copie forensi dei dati, e contestare eventuali ricostruzioni non corrispondenti ai contenuti informativi oggetto del sequestro.

Solo attraverso tali garanzie è possibile scongiurare il rischio di una asimmetria informativa strutturale tra accusa e difesa, e quindi garantire la genuinità del contraddittorio processuale.

5. Il rilievo del controllo giudiziale nella giurisprudenza europea

A rafforzare la necessità del controllo giurisdizionale interviene con chiarezza la giurisprudenza delle Corti europee, che ha indicato il coinvolgimento di un giudice o, in subordine, di un'autorità indipendente, quale condizione imprescindibile per la legittimità delle misure invasive nel trattamento dei dati personali. Tale figura non può essere il pubblico ministero, che, per quanto improntato a un approccio imparziale nella conduzione delle indagini, manca tuttavia del requisito della neutralità, vale a dire della estraneità alla causa (quello che, secondo l'art. 111 Cost è costituito dalla terzietà), dovendo esercitare l'azione penale all'esito della fase investigativa (sul punto si rinvia alle inequivoche osservazioni espresse dalla Corte di giustizia nei casi *Prokuratuur* e *Landek*, menzionati in bibliografia).

Tanto la Corte EDU quanto la Corte di giustizia dell'Unione europea, vale la pena ribadirlo, richiedono che le interferenze sui dati, e in specie nella loro acquisizione massiva, come si verifica attraverso il sequestro di un dispositivo digitale, siano sottoposte a un vaglio effettivo di un soggetto terzo ("neutrale", nella terminologia della Corte di giustizia), volto a verificare la stretta necessità e la proporzionalità della misura, con riferimento alle circostanze concrete del caso. L'assenza di tale controllo espone dunque inevitabilmente l'ordinamento a possibili censure sul piano convenzionale e costituzionale.

In questo senso, la proposta di legge rappresenta una risposta coerente con il diritto europeo, contribuendo a rafforzare le garanzie individuali e a legittimare, anche sul piano democratico, l'azione penale condotta nel contesto digitale.

II. Osservazioni e proposte sul testo normativo in esame

Nel passaggio alla seconda parte della presente analisi, desidero offrire alcuni suggerimenti tecnici volti a migliorare il testo normativo attualmente in discussione, con particolare riferimento alla disciplina contenuta nel nuovo articolo 254-*ter* del codice di procedura penale, nella formulazione proposta dalla legge C. 1822.

Nel suo complesso, la riforma meritoriamente introduce un primo livello di controllo giurisdizionale sulle operazioni di sequestro di dispositivi digitali. Tuttavia, ritengo opportuno sollecitare una riflessione circa l'opportunità di un rafforzamento ulteriore del ruolo del giudice, specie in alcuni snodi critici della disciplina, in cui il potere del g.i.p. rimane, a mio avviso, ancora limitato e potenzialmente non conforme ai paradigmi europei in materia di tutela dei dati personali e di controllo delle misure invasive.

1. Accesso a dati remoti e controllo preventivo del g.i.p.

Il primo punto concerne il comma 6 dell'art. 254-*ter*, che disciplina la possibilità, per le autorità inquirenti, di accedere da remoto — attraverso il dispositivo sequestrato — a dati o programmi informatici collocati in ambienti diversi da quelli fisicamente oggetto di sequestro, come nel caso dei servizi cloud.

Si tratta di una misura particolarmente delicata, poiché permette l'estensione del potere investigativo oltre i limiti fisici del dispositivo sequestrato, potenzialmente verso spazi digitali non previamente individuati, e contenenti dati di terzi o informazioni estranee all'indagine.

Per tale ragione, propongo che **l'accesso remoto venga subordinato a un'autorizzazione preventiva del giudice per le indagini preliminari**. Una simile previsione è coerente sia con i principi della Corte EDU e della Corte di giustizia UE, sia con il generale principio di proporzionalità, che impone un vaglio *ex ante* (nonché un controllo costante *in itinere*) di tutte le misure invasive nella sfera dei dati personali.

2. Deroga alla procedura ordinaria di duplicazione: necessità di autorizzazione *ex ante*

Il secondo profilo critico riguarda il comma 10 dell'art. 254-*ter*, che consente al pubblico ministero, in presenza di talune condizioni di urgenza, di derogare alla procedura ordinaria di duplicazione del dispositivo sequestrato — procedura che, nella sua versione di base, prevede la partecipazione della persona sottoposta a indagini, della persona offesa e dei loro consulenti tecnici.

La deroga è prevista per ipotesi gravi, individuate mediante rinvio agli articoli 406, comma 5-*bis*, e 371-*bis*, comma 4-*bis* c.p.p. Tuttavia, nella formulazione attuale, tale

facoltà è rimessa alla valutazione unilaterale del pubblico ministero, senza la necessità di alcuna autorizzazione o convalida da parte del giudice.

Anche in questo caso, ritengo **opportuno introdurre un controllo *ex ante* del g.i.p.**: è **sufficiente**, **nella stessa istanza con cui il pubblico ministero chiede l'autorizzazione al sequestro del dispositivo** (come già previsto dal comma 1), inserire anche la richiesta di autorizzazione alla deroga alla procedura ordinaria di duplicazione, motivando l'urgenza in relazione a una delle situazioni previste dal comma 10 (pericolo per la vita o l'incolumità di una persona; rischio di cancellazione o dispersione dei dati; concreto pregiudizio per le indagini). Questa integrazione procedurale sarebbe minimale sul piano dell'efficienza, poiché non implica un aggravio burocratico significativo, ma offrirebbe un rilevante presidio di legalità e di tutela, rimettendo al giudice il potere di verifica della reale sussistenza delle condizioni di urgenza. In molti casi, direi nella gran parte, è verosimile che il g.i.p. accolga la richiesta del pubblico ministero; ma si tratta pur sempre di una valutazione giurisdizionale che conferisce maggiore legittimazione e trasparenza all'atto (oltre a prevenire le richieste a prima vista prive di quella urgenza che invece la legge prescrive). In alternativa, si può anche pensare a una validazione giudiziale *ex post*, sempre ad opera del g.i.p., sulla falsariga di quanto già avviene con riferimento alle intercettazioni (art. 267 comma 2 c.p.p.) o alla acquisizione dei dati (art. 132 c. privacy), quando sono disposti d'urgenza dal p.m..

3. La selezione dei dati da parte del pubblico ministero: opportunità di rafforzare la partecipazione delle parti

Un ulteriore profilo meritevole di intervento riguarda la disciplina della selezione dei dati digitali da parte del pubblico ministero, una volta effettuata la duplicazione integrale del dispositivo sequestrato.

Come previsto dai commi 6, 7 e 8 del nuovo art. 254-*ter*, la duplicazione del contenuto del dispositivo deve avvenire in contraddittorio con la persona sottoposta a indagini e, in un assetto ottimale, permettendo la partecipazione la persona offesa, che possono intervenire anche tramite propri consulenti. Tuttavia, una volta completata tale fase tecnica, la selezione dei dati da sottoporre a sequestro viene effettuata in via unilaterale dal pubblico ministero, senza un nuovo momento di partecipazione delle parti.

Questa impostazione, sebbene formalmente corretta, potrebbe essere migliorata al fine di rafforzare le garanzie del contraddittorio e avvicinare il modello italiano a quello già applicato in materia di intercettazioni telefoniche, dove è prevista una forma di selezione in contraddittorio delle conversazioni rilevanti esperibile non appena terminate le operazioni intercettative. In questa prospettiva, suggerisco di valutare, anche per la selezione dei dati rilevanti ottenuti dal dispositivo sequestrato, **l'introduzione di una fase partecipata, immediatamente successiva alla duplicazione, in cui la difesa** (e,

volendo, anche la persona offesa) **sia messa nella condizione di interloquire sulla selezione dei dati da acquisire**, o quantomeno di formulare proposte motivate al pubblico ministero, prima della formalizzazione del decreto di sequestro dei dati individuati. Questa anticipazione del confronto, collocata cronologicamente nel momento più delicato dell'analisi selettiva, garantirebbe una maggiore trasparenza dell'azione investigativa e una più piena valorizzazione del principio di leale collaborazione tra le parti, a vantaggio dell'interesse generale all'accertamento della verità.

In alternativa, si potrebbe intervenire sull'articolo 415-*bis* c.p.p., nella parte in cui viene integrato con il nuovo comma 2-*ter*, al fine di rafforzare le facoltà della difesa nel momento in cui essa prende visione degli atti e formula richieste al termine delle indagini preliminari. In particolare, si propone di introdurre **la possibilità per la difesa di chiedere una proroga fino a trenta giorni** del termine per esaminare il contenuto del dispositivo duplicato, rispetto ai venti giorni attualmente previsti dall'art. 415-*bis*. Tale estensione temporale trova giustificazione nella natura e nel volume potenziale dei dati contenuti nei dispositivi digitali — specialmente se si considera che il sequestro può estendersi anche ai dati accessibili da remoto (es. *cloud*), che ampliano enormemente l'insieme delle informazioni da esaminare.

Occorre inoltre rilevare che la difesa, in tale fase, stando alla proposta di legge in esame, non ha diritto ad ottenere copia integrale dei dati duplicati, ma solo di quelli effettivamente sottoposti a sequestro dal pubblico ministero. Per verificare la sussistenza di ulteriori dati di interesse difensivo, il difensore deve recarsi fisicamente presso gli uffici dell'autorità giudiziaria e consultare *in loco* l'intero contenuto duplicato. In tale contesto, venti giorni possono risultare insufficienti a garantire un'analisi approfondita e un'eventuale richiesta di estensione del perimetro probatorio.

Pertanto, si propone di consentire alla difesa di chiedere una proroga del termine fino a trenta giorni, rimettendo la decisione al pubblico ministero. Qualora quest'ultimo esprima parere contrario, **si potrebbe applicare per analogia il meccanismo previsto dall'art. 368 c.p.p., in base al quale il pubblico ministero trasmette la richiesta al giudice per le indagini preliminari, corredandola del proprio parere**.

Va da sé che, se si opta per un intervento a posteriori da parte della difesa, **tutte le operazioni compiute dal pubblico ministero** (e, se autorizzata, dalla polizia) sul dispositivo duplicato per selezionare i dati ritenuti rilevanti **devono essere accuratamente riportate in un verbale che dia conto degli strumenti usati** (le parole-chiave di ricerca, ad esempio) **per effettuare la selezione**. In questa maniera, la difesa, pur intervenendo successivamente, avrà l'opportunità di poter criticare dialetticamente le scelte di ricerca effettuate dalle autorità inquirenti. Del resto, è la stessa giurisprudenza delle Corti europee ad imporlo: è proporzionato un intervento nel quale **il giudice sia posto in grado di sindacare il modo in cui i dati verranno trattati dagli inquirenti**, e, in particolare, dei **criteri di ricerca che essi intendono adottare** per orientarsi nel *mare magnum* delle informazioni digitali apprese. In sostanza, il giudice deve verificare e

autorizzare ogni selezione sui dati originariamente raccolti, ivi compresa la scelta delle parole-chiave delle quali gli inquirenti intendono avvalersi. Questo controllo, e questo lavoro, per così dire, di "scrematura" dei dati, deve essere messo a disposizione della difesa, nel momento in cui sia possibile la *disclosure*. Quello imposto dalla giurisprudenza europea – vale la pena sottolinearlo – pare un modo di operare di indubbio interesse, posto che, attraverso la verifica dei criteri con i quali l'accusa seleziona progressivamente i dati, il giudice, prima, e la difesa, poi, sono in grado di sindacare il modo nel quale il caso è stato costruito (permettendo così all'imputato, ove necessario, di criticarne i criteri o di integrare le informazioni attraverso una ricerca orientata diversamente, o improntata a criteri selettivi differenti). Sul punto si richiama la sentenza Corte Edu, 25 maggio 2021, *Big Brother Watch e al c. Regno unito*, ric. n. 58170/13, 62322/14 e 24960/15, che specificamente menziona questa necessità.

4. Accesso alla selezione dei dati da parte della persona offesa: estensione nei reati da "codice rosso"

Infine, si propone di riflettere sull'opportunità di garantire un accesso ai dati più effettivo anche alla persona offesa, al termine delle indagini (vale a dire con l'invio dell'avviso di conclusione *ex* art. 415-*bis*), in particolare nei procedimenti relativi a reati di particolare impatto sociale e individuale, come quelli previsti dal c.d. "codice rosso".

Se, da un lato, è comprensibile la necessità di tutelare l'integrità delle indagini, dall'altro, nei procedimenti in cui la persona offesa riveste un ruolo processuale centrale (ad esempio nei reati contro la libertà sessuale, contro la persona o in ambito familiare), appare ragionevole prevedere un diritto di intervento, anche differito o sotto forma di osservazioni, nella fase di selezione dei dati, eventualmente da esercitare con l'assistenza di un proprio consulente tecnico.

Tale estensione rafforzerebbe la dimensione inclusiva e partecipativa del processo penale contemporaneo, nel rispetto delle garanzie di imparzialità e riservatezza.

5. Perquisizioni informatiche e antinomia sistemica: la necessità di una autorizzazione preventiva del giudice

Un ultimo — ma strutturalmente decisivo — profilo critico riguarda la disciplina delle perquisizioni informatiche, che la proposta di legge intende modificare mediante l'aggiunta di un comma 1-*bis* all'art. 247 c.p.p.

Nella formulazione attuale del disegno di legge in discussione, il potere di disporre la perquisizione di un dispositivo digitale continua a rimanere esclusivamente affidato al pubblico ministero, tramite decreto motivato. Il giudice per le indagini preliminari interviene, secondo il nuovo testo, solo in due casi:

1. se, all'esito della perquisizione, il pubblico ministero ritiene necessario procedere al sequestro dell'intero dispositivo (art. 254-*ter*, comma 1);
2. se intende sequestrare dati inerenti a comunicazioni (art. 254-*ter*, comma 12).

Pur rappresentando uno sforzo apprezzabile di rafforzamento delle garanzie, questa impostazione resta insufficiente rispetto al quadro di principi che dovrebbe regolare la materia, in conformità al diritto costituzionale ed europeo. Infatti, se si mantiene l'attuale formulazione dell'art. 247 c.p.p., **si genera un meccanismo alternativo - e dunque potenzialmente elusivo - rispetto alla disciplina prevista dal nuovo art. 254-*ter***. Il pubblico ministero potrà, in astratto, scegliere tra due percorsi paralleli per ottenere l'accesso e la duplicazione dei dati contenuti in un dispositivo digitale:

- o chiedere, prima di procedere alla perquisizione, fin da subito al g.i.p. l'autorizzazione al sequestro dell'intero dispositivo, attivando così la procedura ordinaria prevista dall'art. 254-*ter* c.p.p., con tutte le garanzie partecipative e tecniche ivi previste;

- oppure, procedere autonomamente alla perquisizione informatica, attenendosi a quanto prescritto dall'art. 247 c.p.p. (vale a dire adottando misure tecniche tali da assicurare la non alterazione e la conservazione dei dati originali), riservandosi semmai di chiedere il provvedimento del g.i.p. in un momento successivo, quando intenda procedere al sequestro del dispositivo.

Il paradosso, tuttavia, è che questa seconda possibilità (effettuare la perquisizione informatica, riservandosi a un momento futuro la scelta se procedere al sequestro), di fatto, inevitabilmente, implica già una duplicazione del dispositivo (e dunque un sequestro dello stesso, in via di fatto). Non v'è altro modo, infatti, di assicurare quella non alterazione e conservazione dei dati originali, pretesa dall' dell'art. 247 c.p.p., se non attraverso l'effettuazione di una copia conforme del *digital device*: l'operazione è la stessa, sul piano tecnico, di quella descritta all'art. 254-*ter* c.p.p., ma, nel caso della semplice "perquisizione" informatica, essa è preceduta di fatto, se non si vuole compromettere lo stato originale dei dati, da una sorta di sequestro e duplicazione materiale, al di fuori delle garanzie introdotte con il nuovo articolo del codice.

In sostanza, se non si corregge l'art. 247 comma 1-*bis* c.p.p., che, al momento, consente al pubblico ministero di perquisire un dispositivo, con modalità tali da non alterarne il contenuto originale (e dunque implicitamente imponendo al magistrato inquirente la duplicazione del contenuto con copia digitale conforme), si immette un'ambiguità sistemica: la duplicazione di un dispositivo digitale - che è sempre necessaria sul piano tecnico per poterlo poi perquisire senza introdurre alterazioni fatali – può (anzi, deve) già adesso avvenire *secundum legem* sulla base del solo provvedimento del p.m., *ex* art. 247 comma 1-*bis* c.p.p. Così, tuttavia, in prospettiva, ove fosse approvato il nuovo art. 254-

ter c.p.p., si finirebbe per consentire una "legittima" elusione del controllo giudiziale preventivo e della partecipazione delle parti, che dovrebbe essere imposta dal nuovo articolo inserito nel codice. Di fatto, quindi, **la disciplina delle perquisizioni informatiche (art. 247 c.p.p.) rischia di vanificare le garanzie che si desidera introdurre proprio con l'art. 254-*ter* c.p.p., consentendo una forma surrettizia di duplicazione e analisi dei dati digitali senza autorizzazione giudiziaria e senza contraddittorio**.

Per evitare questa frattura normativa e garantire coerenza sistemica, **si propone che l'art. 247 c.p.p. venga modificato prevedendo, in via generale, che ogni perquisizione di un dispositivo digitale debba essere preceduta da un'autorizzazione del giudice per le indagini preliminari**. In tal modo, verrebbe riconosciuta la natura intrinsecamente invasiva di ogni perquisizione informatica, e si escluderebbe la possibilità che essa si traduca in una duplicazione di fatto, non sorvegliata e potenzialmente non tracciabile.

Questa modifica avrebbe l'effetto di riordinare l'intera materia su un asse coerente: ogni accesso ai dati digitali, che sia funzionale alla loro duplicazione, alla perquisizione o al sequestro, richiederebbe un vaglio giudiziale *ex ante*, assicurando il rispetto dei principi di legalità, necessità e proporzionalità, conformemente agli standard convenzionali.

La necessità di coinvolgere il giudice per le indagini preliminari in maniera sistematica non è una rigidità procedurale, ma una scelta coerente con lo sviluppo della modernità giuridica e tecnologica. Accedere ai dati digitali di un individuo rappresenta oggi un'operazione di estrema delicatezza, paragonabile — per profondità intrusiva e sensibilità dei contenuti — alle intercettazioni di comunicazioni. In molti casi, l'analisi dei dati digitali consente di ricostruire la sfera intima della persona in modo persino più dettagliato e pervasivo di quanto non faccia un singolo frammento di conversazione captata.

Di fronte a questa realtà, le sentenze delle Corti europee ci indicano con chiarezza la necessità di un adattamento del sistema: l'intervento del g.i.p. non può più essere concepito come misura eccezionale o eventuale, ma deve assumere carattere strutturale in tutte le situazioni che implichino un'ingerenza significativa nella vita privata.

Va da sé, infine, che anche gli articoli 352 e 354 c.p.p. debbano essere riformati, prevedendo che, nei casi in cui le perquisizioni o i sopralluoghi di iniziativa della polizia giudiziaria abbiano ad oggetto dispositivi digitali, la comunicazione al pubblico ministero sia seguita da una richiesta di convalida al giudice, secondo lo schema già delineato dal nuovo art. 254-*ter*, comma 4.

Conclusioni

Le proposte qui presentate proposte muovono tutte nella direzione di un rafforzamento delle garanzie del procedimento, senza sacrificare le esigenze di efficienza investigativa (o sacrificandole nella misura strettamente necessaria). Al contrario, un impianto normativo chiaro, ordinato e bilanciato contribuisce a consolidare la legittimità delle attività d'indagine, prevenendo conflitti interpretativi e contenziosi futuri.

Il diritto processuale penale - soprattutto adesso, nel pieno della rivoluzione digitale - richiede un equilibrio nuovo tra efficienza e tutela, tra poteri d'indagine e diritti della persona. È compito del legislatore, attraverso interventi mirati e rigorosi, riempire di contenuto sostanziale i principi dello Stato di diritto nell'era digitale.

In questa chiave di lettura, la riforma che ha come centro l'art. 254-*ter* può essere considerata come un passo significativo verso la regolazione delle indagini digitali, un tema che, complessivamente, necessità di un intervento normativo (si pensi alle questioni irrisolte del pedinamento elettronico, dell'uso del captatore informatico (*trojan*) per fini diversi da quelli di intercettazione, e ai diversi usi in ambito probatorio – oltre che decisorio – cui si presta già ora l'intelligenza artificiale).

Bibliografia essenziale

- Sentenze della Corte di giustizia dell'Unione europea
  - 8 aprile 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, ECLI:EU:C:2014:238
  - 21 dicembre 2016, *Tele 2 and Sverige*, C-203/15 and C-698/15, ECLI:EU:C:2016:970
  - 2 ottobre 2018, *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788
  - 6 ottobre 2020, *La Quadrature du Net and others*, C 511/1, C 512/18, C 520/18, ECLI:EU: C:2020:791
  - 2 marzo 2021, *Prokuratuur*, C-746/18, ECLI:EU:C:2021:152
  - 7 settembre 2023, C-162/22 ECLI:EU:C:2023:631
  - 30 aprile 2024, C-178/22, ECLI:EU:C:2024:371
  - 4 ttobre 2024, *Landek*, C-548/21, ECLI:EU:C:2024:830

- Sentenze della Corte europea dei diritti dell'uomo (selezione)
  - 4 dicembre 2015, *Zakharov v. Russia*, *Appl. no.* 47143/06

- 25 maggio 2021, *Big Brother Watch and Others V. The United Kingdom*, Appl. nos. 58170/13, 62322/14 and 24960/15)

- Sentenze della Suprema Corte di cassazione (selezione)
  - Cass., Sez. 6, 9 dicembre 2020, Pessotto (n. 6623 del 2021).
  - Cass., Sez. 6, 21 maggio 2024, Donnarumma, n. 31180.
  - Cass., sez. 6, 15 febbraio 2024, Corsico, n. 17312.
  - Cass., Sez. 6, 22 settembre 2020, Aleotti, n. 34625

- Sentenze della Corte costituzionale italiana (selezione)
  - sentenza 7-22 giugno 2023, n. 170

- Contributi dottrinari (selezione)

  - M. Caianiello – A. Camon (eds), *Digital Forensic Evidence. Towards Common European Standards in Antifraud Administrative and Criminal Investigations*, Cedam, Padova, 2021
  - M. Caianiello, *Dangerous Liaisons. Potentialities and Risks Deriving from the Interaction between Artificial Intelligence and Preventive Justice*, in *European Journal of Crime, Criminal Law & Criminal Justice*, 2021, p. 1 s.
  - A. Chelo, *Tanto tuonò che piovve: il nuovo sequestro di dispositivi informatici*, in *Rivista penale. Diritto e procedura – Riv. trim*., 2024, p. 29 s.
  - J. Della Torre, *L'acquisizione dei tabulati telefonici nel processo penale dopo la sentenza della Grande Camera della Corte di Giustizia UE: la svolta garantista in un primo provvedimento del g.i.p. di Roma*, in *Sistema penale*, 29 aprile 2021
  - J. Della Torre (con A. Malacarne), *L'utilizzo dei file di log per scopi di contrasto alla criminalità: nodi problematici e possibili soluzioni*, in *Archivio penale web*, 2023, n. 3, p. 1 s.
  - F. Dinacci, *I modi acquisitivi della messaggistica chat o email: verso letture rispettose dei principi*, in *Arch. pen*., 2024, p. 1 s.
  - M. Gialuz, *Intelligenza artificiale e diritti fondamentali in ambito probatorio*, in AA.VV., *Giurisdizione penale, intelligenza artificiale ed etica del giudizio, Giuffrè, Milano, 2021, p. 51 s.*
  - G. Lasagni, *Admissibility of Evidence in Criminal Proceedings: Lessons (and Problems) from the "Data Retention Saga"*, in L. Bachmaier Winter – F. Salimi (eds), *Admissibility of Evidence in EU Cross-Border Criminal Proceedings. Electronic Evidence, Efficiency and Fair Trial Rights*, Hart, 2024, p. 35.

- G. Lasagni, *Dalla riforma dei tabulati a nuovi modelli di integrazione fra diritti di difesa e tutela della privacy*, in *Legisl. pen.*, 2022, p. 8.
- S. Marcolini, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen.*, 2015, p. 760 s.
- I. Neroni Rezende, *Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective*, in *The New Journal of European Criminal Law*, 2020, p. 375 s.
- F. Nicolicchia, *A passi incerti nel solco di categorie evanescenti: riflessioni a partire dalla querelle giurisprudenziale sull'acquisizione di messaggistica criptata all'estero*, in *Sistema penale*, 2024, p. 189 s.
- J. J. Oerlemans and D.A.G. van Toor, *Legal Aspects of the EncroChat Operation: A Human Rights Perspective*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 2022, p. 309 s.
- J. J. Oerlmans – S. Royer, *The future of data-driven investigations in light of the Sky ECC operation*, in *New Journal of European Criminal Law*, 2023, p. 447.
- M. Panzavolta – E. Maes, *Exclusion of evidence in times of mass surveillance. In search of a principled approach to exclusion of illegally obtained evidence in criminal cases in the European Union*, in *New Journal of European Criminal Law*, 2022, p. 199 s.
- L. Parodi, *L'uso obliquo dei dati esterni delle comunicazioni tra espansione delle garanzie sovranazionali, inerzia del legislatore e incertezze interpretative*, in *Legisl. pen.*, 2024.
- S. Quattrocolo, *Processo penale e rivoluzione digitale: da ossimoro a endiadi?*, in *MediaLaws*, 2020, p. 121 s.
- S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings: A Framework for a European Legal Discussion*, Spirnger, 2020.