



**Audizione dell'Unione delle Camere Penali Italiane dinanzi alla "II Commissione Giustizia"
della Camera dei Deputati.**

Seduta di mercoledì 27 maggio 2025

Disposizioni in materia di sequestro di dispositivi informatici

PDL già approvata in Senato in data 10 aprile 2024

La PDL in discussione dinanzi la Commissione Giustizia della Camera, con l'inserimento dell'art. 254 *ter* nel codice di rito, intende introdurre una disciplina specifica per il sequestro di dispositivi e sistemi informatici o telematici, memorie digitali, dati, informazioni, programmi, comunicazioni e corrispondenza informatica inviate o ricevute. La nuova disposizione è ispirata dalla condivisa esigenza di tutelare la riservatezza dei dati altamente sensibili contenuti nei dispositivi informatici di uso corrente, quali smartphone, tablet o personal computer, nelle cui memorie sono conservate le tracce di comunicazioni e conversazioni tra privati, intercorse mediante varie tipologie di messaggistica telematica o caselle di posta elettronica (oltre che messaggi audio, immagini e video).

Si tratta di contenuti meritevoli di protezione, secondo quanto stabilito dalla Direttiva UE 2016/680 del 27 aprile 2016, come interpretata dalla Corte di Giustizia dell'Unione europea, Grande Camera, con la recente sentenza del 4 ottobre 2024, C-548/21, successiva rispetto all'approvazione della proposta di legge in Senato, avvenuta in data 10 aprile 2024.

La Direttiva 2016/680 prevede *"norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica"*.

A tale Direttiva è stata data attuazione nell'ordinamento interno con il D.lgs. n. 51 del 18 maggio 2018, che ne ha sostanzialmente riprodotto le previsioni.

La Corte di Giustizia UE, con la suindicata sentenza, ha esteso le disposizioni della Direttiva 2016/680 al trattamento dei dati personali conseguenti al sequestro.

La Corte ha precisato che l'art. 3.2 della Direttiva definisce la nozione di *"trattamento"* come comprendente *"qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come l'estrazione, la consultazione"* o ancora *"la diffusione o qualsiasi altra forma di messa a disposizione"*.

Il successivo art. 4 stabilisce che *"Gli Stati membri dispongono che i dati personali siano: a) trattati in modo lecito e corretto; b) raccolti per finalità determinate, esplicite e legittime e trattati in modo non incompatibile con tali finalità; c), adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono stati trattati"*.

Secondo la Corte, il legislatore dell'Unione europea ha inteso attribuire una portata ampia alla nozione di *"trattamento"*, nel cui ambito rientra anche "un tentativo di accesso ai dati contenuti in un telefono cellulare, da parte dell'autorità di polizia ai fini di una indagine in materia penale".

Unione Camere Penali Italiane

Via del Banco di S. Spirito, 42 00186 Roma

Tel +39 06 32500588 - segreteria@camerepenali.it - www.camerepenali.it

C.F. 05386821002 - P.I. 08989681005



“Infatti, ai sensi dell’art. 4, paragrafo 1, lett. b), di tale direttiva, gli Stati membri dispongono che i dati personali siano raccolti per finalità determinate, esplicite e legittime e trattati in modo non incompatibile con tali finalità. Orbene, l’effettività di tale principio esige necessariamente che la finalità della raccolta sia determinata dalla fase in cui le autorità competenti tentano di accedere a dati personali, poiché un siffatto tentativo, qualora si riveli proficuo, è tale da consentire a tali autorità, in particolare, di raccogliere, estrarre o consultare immediatamente i dati in questione” (sent. Corte di Giustizia UE pag. 73).

La Direttiva in esame, sempre secondo la Corte, consente il trattamento dei dati, inteso nel senso sopra indicato, nell’ambito di una indagine diretta alla repressione di un reato, a condizione che, in primo luogo, la limitazione dei diritti fondamentali al rispetto della vita privata e alla protezione dei dati di carattere personale che esso necessariamente implica sia “necessaria” e “tale requisito non è soddisfatto quando l’obiettivo di interesse generale perseguito sia ragionevolmente conseguibile in modo altrettanto efficace con altri mezzi, meno pregiudizievoli” (sent. Corte di Giustizia UE pag. 87).

In secondo luogo, la limitazione suddetta deve essere prevista dalla legge, requisito che implica che “la base giuridica che autorizza una simile limitazione ne definisce la portata in modo sufficientemente chiaro e preciso” e, infine, deve rispettare il criterio di proporzionalità, insito nella previsione di cui all’art. 4, lett. c), che richiede il rispetto, da parte degli Stati membri, del principio di “minimizzazione dei dati”, che di quel criterio costituisce espressione (sent. Corte di Giustizia UE pag. 79).

Al fine di garantire che i presupposti per il trattamento dei dati siano rispettati, è necessario che l’accesso “sia subordinato a un controllo preventivo effettuato da un giudice o da un organo amministrativo indipendente” (pag. 102).

In sostanza, la Corte di Giustizia UE ha ritenuto che il trattamento di dati personali, inteso in senso ampio, debba essere autorizzato da un giudice o da un organo amministrativi indipendente.

Con specifico riferimento all’individuazione, nell’ordinamento interno, dell’organo legittimato al controllo relativo alla eventuale sussistenza dei presupposti per l’accesso ai dati contenuti in un dispositivo informatico, la Sesta Sezione della Corte di cassazione, con la recente sentenza n. 413 dell’1° aprile 2025 (proc. n. 41555/2024 R.G.), ha escluso che tale funzione di controllo (giudice o organo amministrativo indipendente, secondo la Corte di Giustizia UE) possa essere esercitata dal pubblico ministero, “per la sua natura di parte processuale, a prescindere dal suo statuto di autonomia”.

Ciò premesso, la proposta di legge in esame, pur essendo certamente migliorativa, sul piano delle garanzie e della tutela dei diritti fondamentali del cittadino, presenta alcuni aspetti distonici rispetto ai richiamati principi di matrice sovranazionale.

Il testo dell’art. 254 *ter* già licenziato dal Senato risulta piuttosto ampio prevedendo due diversi step autorizzativi, uno preliminare, disciplinato dal primo comma, che riguarda il sequestro dei dispositivi, ed uno, eventualmente successivo all’analisi del duplicato informatico, disciplinato dal comma 12.



In particolare, su richiesta del P.M., il Gip dispone, con decreto motivato, il sequestro dei “dispositivi” necessari per la prosecuzione delle indagini in relazione alle circostanze di tempo e di luogo del fatto e alle modalità della condotta, nel rispetto del criterio di proporzione, trasmettendo immediatamente il provvedimento al P.M., che ne dovrà curare l’esecuzione (comma 1).

Successivamente, dopo la fase relativa alla duplicazione del contenuto, il comma 12 prevede:

- a) un ulteriore decreto motivato, di competenza del P.M., che dispone il sequestro dei dati, delle informazioni e dei programmi strettamente pertinenti al reato;
- b) un regime autorizzativo simile a quello previsto per le intercettazioni (articoli 266 comma 1 e 267 comma 1), qualora il pubblico ministero intenda procedere al sequestro dei dati inerenti a comunicazioni, conversazioni o corrispondenza informatica inviate e ricevute.

Andrebbe, in ogni caso, richiamato il anche il comma 1 bis dell’art. 267, non indicato al comma 12, poiché ai fini della valutazione dei gravi indizi di reato non può non trovare applicazione l’art. 203 c.p.p.

Le ulteriori facoltà, successive all’analisi del duplicato informatico del contenuto, consentono l’accesso ai dati sulla base di presupposti invero piuttosto generici ed indefiniti, quali la “necessità” per la prosecuzione delle indagini in relazione alle circostanze di tempo e di luogo del fatto e alle modalità della condotta, nel rispetto del criterio di proporzione, la cui delimitazione risulta eccessivamente aleatoria, lasciando eccessivi margini di discrezionalità all’Autorità Giudiziaria procedente.

Tali circostanze si pongono in contrasto, non solo con i principi costituzionali, ma anche con le più recenti indicazioni giurisprudenziali della Corte di cassazione, con specifico riferimento all’illegittimità del sequestro a fini probatori di una indistinta massa di dati informatici, con una indiscriminata apprensione di tutte le informazioni ivi contenute, in difetto di specifiche ragioni (cfr. Cass. Sentenze n. 38460 del 27.10.2021 e n. 17604 del 2023), e della richiamata sentenza della Corte di Giustizia UE, secondi cui i presupposti richiesti per l’accesso devono essere definiti in modo sufficientemente chiaro e preciso.

Nel caso di specie, il primo comma dell’art. 254 ter, oltre a richiamare il rispetto al criterio di proporzione, si limita a menzionare genericamente solo il requisito della “necessità”, ai fini della prosecuzione delle indagini, mentre nulla dice in ordine all’ulteriore presupposto dell’“esclusività” del sequestro, rispetto ad altri mezzi di ricerca della prova.

La parte del comma 12 che attribuisce al P.M. il potere di disporre autonomamente il sequestro di una serie di dati, solo apparentemente diversi (si pensi ad esempio allo screenshot di un messaggio whatsapp) da quelli rappresentativi di comunicazioni, conversazioni o corrispondenza informatica, si pone, altresì, in contrasto con la prescrizione comunitaria, secondo cui l’accesso ai dati sensibili può essere autorizzato esclusivamente da un giudice o da una autorità amministrativa indipendente.

Il doppio regime autorizzativo, sequestro del dispositivo e successiva acquisizione (per l’utilizzazione) dei dati, appare effettivamente superfluo attesa la sostanziale inscindibilità investigativa tra le due/tre operazioni, in quanto tutte finalisticamente orientate ad accedere ai



contenuti, pacificamente coincidenti con dati altamente sensibili, soggetti alla massima tutela, sia nell'ordinamento costituzionale interno che sul versante sovranazionale.

Pertanto, anche in considerazione della *ratio legis* fondata sulla necessità di fornire una disciplina capace di riequilibrare il rapporto tra il rispetto dei diritti individuali, costituzionalmente e convenzionalmente riconosciuti, e le esigenze investigative, sarebbe auspicabile sottoporre il sequestro dei dispositivi informatici e dei relativi contenuti alle regole previste per le intercettazioni di conversazioni o comunicazioni, certamente più aderenti ai presupposti richiesti dalla Direttiva UE 2016/680 del 27 aprile 2016, come interpretata dalla Corte di Giustizia dell'Unione Europea con la sentenza del 4 ottobre 2024, C-548/21.

In sostanza, il sequestro dovrebbe essere disposto dal Giudice, su richiesta del P.M. (ovvero, nei comprovati casi di urgenza, col meccanismo della successiva convalida da parte del Giudice), a pena di inutilizzabilità, come già si desume, solo per uno dei due successivi passaggi relativi all'acquisizione dei dati, dalla parte del comma 12 riguardante il sequestro di comunicazioni, conversazioni o corrispondenza informatica, mediante il rinvio alla disciplina prevista in tema di intercettazioni (art. 266, comma 1, e 267, comma 1), nonché dal richiamo operato dal comma 14 alle disposizioni di cui agli artt. 103, 270 e 271 c.p.p.

Un così articolato regime autorizzativo rivestirebbe un ulteriore pregio, poiché eviterebbe problemi interpretativi successivi, relativi alla distinzione tra comunicazioni e meri documenti, con riferimento, a titolo esemplificativo, alla classificazione di uno *screenshot* di un dialogo intercorso sull'applicativo whatsapp (anche tramite lo scambio di messaggi "vocali"), quale corrispondenza o documento/fotografia, che si riverbera automaticamente sulle modalità procedurali di acquisizione del dato.

I presidi di garanzia proposti sono finalizzati, da un lato, a prevenire il rischio di trasformare il sequestro da mezzo di ricerca della prova a mezzo di ricerca di ulteriori notizie di reato e, dall'altro, a restringere a monte i casi di accesso ad una copiosa mole di dati privati altamente sensibili, considerato che un intervento del Giudice finalizzato all'esclusione dei dati non rilevanti o, comunque, potenzialmente lesivi della riservatezza di tutti i soggetti coinvolti, è previsto dal comma 17 solo in un momento successivo rispetto alla duplicazione informatica dei contenuti ed alla estrapolazione dei dati.

Rispetto ai testi esaminati in Commissione Giustizia al Senato, quello approvato dal medesimo ramo del Parlamento risulta certamente più efficace in relazione al regime delle inutilizzabilità.

Ferma restando la necessità di inserire anche i divieti previsti dall'art. 203 c.p.p., espressamente richiamato in materia di intercettazioni dall'art. 267 comma 1 bis, il comma 14 introduce l'applicabilità delle disposizioni previste dall'art. 103 c.p.p. in tema di garanzie di libertà del difensore, rafforzate dalla novella introdotta dalla legge n. 114 del 9 agosto 2024, con particolare riferimento al rafforzamento del divieto di intercettazioni di tutte le forme di corrispondenza e comunicazione che intervengono tra il difensore medesimo e il proprio assistito.

L'ulteriore rinvio alle disposizioni previste dall'art. 270, commi 1 e 2, e dall'art. 271 c.p.p., consente sia l'applicabilità dei limiti previsti per l'utilizzo dei risultati delle acquisizioni in altri procedimenti, che i divieti di utilizzazione stabiliti in materia di intercettazioni.



In particolare, rispetto alla criticità relativa al mancato richiamo dell'art. 203 c.p.p. nel testo del comma 12, il rinvio integrale che il comma 14 opera in relazione all'art. 271 c.p.p. potrebbe far ritenere colmata la predetta lacuna.

A tal proposito, l'unico ostacolo interpretativo potrebbe desumersi dall'inciso "*in quanto compatibili*", inutilmente e poco comprensibilmente contenuto proprio nel testo del comma 14.

Tornando alla seconda parte del comma 12, non è condivisibile l'inserimento dell'attenuazione del presupposto dei gravi indizi di reato, sostituito con i sufficienti indizi, mediante il rinvio all'art. 13 del D.L. 152/91 convertito con la legge n. 203/91 (c.d. regola del doppio binario, la cui continua espansione è ampiamente censurabile, poiché allontana sempre di più il nostro sistema penale dai principi costituzionali che lo governano), in primo luogo, per ragioni di carattere generale connesse ai principi costituzionali (presunzione di non colpevolezza, natura personale della responsabilità penale, tutela delle libertà fondamentali e principio di uguaglianza su tutti) in base ai quali l'indagine e l'intero procedimento penale devono essere parametrati sulla figura dell'indagato/imputato, prescindendo dall'ipotesi di reato, la cui eventuale sussistenza è, appunto, demandata esclusivamente all'accertamento processuale.

Sotto altro profilo, in particolare, l'applicazione della regola del doppio binario risulta sproporzionata poiché, trattandosi di un generalizzato accesso ex post alla vita privata del cittadino, la dimensione della gravità indiziaria in ordine alla sussistenza di un reato appare decisamente un requisito minimale per giustificare un intervento così invasivo.

Le medesime considerazioni dovrebbero condurre all'abrogazione integrale del comma 10, poiché le esigenze di urgenza, finalizzate a preservare la conservazione e l'integrità del mezzo di prova, sono garantite dalla previsione inserita nel comma 4, che disciplina i casi in cui la polizia giudiziaria ha facoltà di procedere direttamente al sequestro del dispositivo, che dovrà essere successivamente convalidato dal Gip, su richiesta del P.M., qualora sussistano i presupposti.

Il procedimento finalizzato alla duplicazione del contenuto del dispositivo oggetto di sequestro (comma 6), infine, dovrebbe essere disciplinato dalle regole previste dall'art. 360 c.p.p., ivi compresa la riserva di incidente probatorio, atteso che, oltre ad essere già ampiamente utilizzate nella prassi applicativa, risultano, nell'assetto normativo attuale, le più adeguate a garantire il diritto di difesa.

Roma, 27 maggio

La Giunta