IL CONTROLLO GIURISDIZIONALE SUL SEQUESTRO PROBATORIO DI DISPOSITIVI E DATI DIGITALI NELLA GIURISPRUDENZA DI LEGITTIMITÀ: ANAMORFOSI DI UNA GARANZIA

di Massimo Bolognari

La Corte di giustizia ha stabilito che il sequestro probatorio di un dispositivo digitale e del suo contenuto debba essere subordinato ad un controllo giurisdizionale preventivo. Potenzialmente dirompenti le ricadute di tale pronuncia sul nostro ordinamento, che attribuisce al p.m. e, nei casi d'urgenza, anche alla polizia giudiziaria, il potere di disporre una simile misura. Dal canto suo, la cassazione ha negato che il sequestro debba essere autorizzato dal giudice, adottando delle soluzioni interpretative che, pur tentando un 'dialogo' con la sentenza della Corte di giustizia, ne svuotano nella sostanza la portata precettiva. Il presente lavoro ricostruisce i vari orientamenti riscontrabili nella giurisprudenza di legittimità, segnalandone i limiti e le contraddizioni, e si interroga sulle possibili conseguenze processuali del mancato adeguamento a tale pronuncia, tentando, infine, di formulare alcune proposte de iure condendo.

SOMMARIO: 1. Il progressivo potenziamento in via pretoria delle garanzie in materia di sequestro probatorio di dispositivi e dati digitali. – 2. Il controllo giurisdizionale preventivo: una garanzia di matrice europea e i (dis)orientamenti della giurisprudenza di legittimità. – 3. La logica paternalistico-inquisitoria: il pm come autorità amministrativa indipendente. – 4. La logica compensativa: il tentativo di controbilanciare l'assenza di un controllo giurisdizionale *ex ante* con la possibilità di esperire il rimedio del riesame. – 5. La logica 'riduttiva': l'applicazione del previo controllo giurisdizionale al solo accesso ai dati. – 6. Le conseguenze processuali della mancata previsione di un controllo giurisdizionale *ex ante*. – 7. I limiti di un rafforzamento del controllo giurisdizionale. – 8. Scenari *de iure condendo*.

1. Il progressivo potenziamento in via pretoria delle garanzie in materia di sequestro probatorio di dispositivi e dati digitali.

Da tempo si lamenta l'inadeguatezza delle norme che disciplinano il sequestro probatorio di dispositivi e dati digitali[1]. Frutto del recepimento con l. 18 marzo 2008, n. 48 dell'ormai datata Convenzione del Consiglio d'Europa sulla criminalità informatica del 2001[2] e di minimi – e assai poco significativi – interventi successivi[3], tali previsioni

[1] In tal senso, *ex multis*, BARTOLI (2018), pp. 1 ss.; CHELO (2022), pp. 1588 ss.; CURTOTTI (2024), pp. 2703; DELLA TORRE (2025); DINACCI (2025); LASAGNI (2018), pp. 393 ss.; MALACARNE (2025b), pp. 131 ss.; MURRO (2024a), pp. 253 ss.

[2] Grazie al quale sono state innestate nel tessuto codicistico alcune specifiche clausole che tengono conto delle peculiarità del sequestro informatico, come il dovere di assicurare l'immodificabilità e la conservazione dei dati digitali, nonché il divieto di alterazione dei medesimi e l'obbligo di realizzare una copia di essi conforme all'originale. Per un esame di tali prescrizioni, v., per tutti, SIGNORATO (2018), pp. 134 ss.

[3] Si pensi, ad esempio, al d.lgs. 30 dicembre 2025, n. 215, che, nel recepire il regolamento 2023/1543/UE relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche nei

Editore Associazione "Progetto giustizia penale" | via Festa del Perdono 7, 20122 Milano
c/o Università degli Studi di Milano, Dipartimento di Scienze Giuridiche "Cesare Beccaria"
redazione@sistemapenale.it

non risultano solo inadatte a regolare fenomeni che presentano una sempre più accentuata complessità[4], ma accordano anche una tutela insufficiente alle persone destinatarie di simili provvedimenti ablativi[5]. Si tratta di un deficit particolarmente allarmante, se si considera che quest'ultimi sono suscettibili di comprimere garanzie fondamentali[6]. Accanto al diritto di proprietà (art. 42 Cost. e art. 1 Primo Protocollo addizionale alla Cedu), vengono in rilievo la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione (15 Cost.), il diritto alla riservatezza, che, pur non trovando un'esplicita enunciazione nella Costituzione, viene tutelato dall'art. 8 Cedu e dall'art. 7 della Carta dei diritti fondamentali dell'Unione europea (d'ora in poi "Carta"), e il diritto alla protezione dei dati personali (art. 8 Carta)[7]. A colmare – quantomeno in parte – un simile vuoto di tutela è intervenuta la giurisprudenza di legittimità, che nel tempo ha elaborato una serie di regole funzionali a garantire che l'acquisizione di dispositivi e dati informatici avvenga in conformità al principio di proporzionalità[8] e sia

---

procedimenti penali, ha inserito nel codice all'interno delle norme dedicate al sequestro probatorio un nuovo art. 263 bis c.p.p., in base al quale il p.m. può disporre con decreto motivato che i fornitori e gli operatori di servizi informatici, telematici o di telecomunicazioni conservino e proteggano i dati che essi detengono per un periodo non superiore a novanta giorni.

[4] Cfr. SIGNORATO (2018), pp. 131-132, la quale evidenzia, più in generale, come le soluzioni adottate dal legislatore con l. 48/2008 fossero nel complesso insoddisfacenti, traducendosi non tanto in un ripensamento complessivo del sistema dei mezzi di ricerca della prova alla luce delle innovazioni derivanti dal progresso tecnologico, quanto piuttosto di un adattamento degli strumenti tradizionali.

[5] Si pensi, ad esempio, alla mancata valorizzazione a livello normativo del principio di proporzionalità, che potrebbe, invece, giocare un ruolo cruciale in questo contesto, essendo uno strumento che è concepito "quale argine e canone di legittimazione di ogni invasione delle prerogative individuali da parte dello Stato" e che, al contempo, consente di incanalare "il lavoro giudiziale verso un alveo razionale standardizzato": così, CAIANIELLO (2014), p. 143.

[6] Come evidenziato anche da TORRE (2026), pp. 506-507.

[7] Ma potrebbe venire in gioco pure il c.d. "domicilio informatico". Secondo alcuni, tale concetto sarebbe ricavabile dall'art. 14 Cost. (cfr., tra gli altri, CAMON (2017), p. 95; CAPRIOLI (2017), p. 490; PARLATO (2018), p. 302), mentre altri, qualificandolo diversamente come diritto all'uso confidenziale dei sistemi informatici, lo riconducono all'art. 2 Cost. (Cfr. ORLANDI (2018), pp. 540 ss., il quale fa risalire l'origine di questa garanzia ad un'importante pronuncia del 2008 della Corte costituzionale tedesca).

[8] Principio che, pur essendo esplicitamente richiamato nel codice di rito solo nell'ambito delle norme che regolano le misure cautelari, possiederebbe una particolare forza espansiva, assumendo portata generale e trovando, dunque, applicazione anche alla materia probatoria. In particolare, la Cassazione ne ha esteso il raggio d'azione anche al sequestro: cfr., in particolare, Cass., Sez. un., 28 gennaio 2004, n. 5876, secondo la quale le operazioni acquisitive devono riguardare beni concretamente necessari alle finalità probatorie, essendo indispensabile che nella motivazione del provvedimento compaiano le ragioni che giustificano il vincolo, e Cass., Sez. un., 19 aprile 2018, n. 36072, che ha evidenziato come tale misura ablativa possa essere disposta solo quando non sia possibile conseguire il medesimo risultato con modalità meno afflittive. Dal canto loro, la Corte di giustizia e la Corte europea dei diritti dell'uomo, a partire rispettivamente dalle note sentenze *Digital Rights Ireland* e *Zacharov c. Russia*, hanno dato un impulso decisivo all'applicazione del principio di proporzionalità nell'ambito dell'acquisizione delle prove digitali nella prospettiva di assicurare un adeguato contemperamento tra le esigenze investigative e la protezione dei diritti fondamentali. A tal fine, la giurisprudenza europea, nei confronti della quale, come si vedrà, la Cassazione ha mostrato una certa sensibilità, impone che le misure che implicano un'intrusione nella sfera individuale trovino un loro fondamento in una base giuridica adeguata, che stabilisca i casi e le tipologie di reato per le quali è possibile disporle, e siano assoggettate al controllo del giudice, il quale deve verificare l'esistenza di una giustificazione fattuale dell'atto istruttorio e l'indisponibilità di strumenti meno invasivi che siano in grado

rispettosa dei diritti fondamentali[9]. Si tratta di una sorta di protocollo operativo nel quale è possibile ricomprendere, per un verso, specifici oneri motivazionali in capo al p.m. che dispone la misura ablativa e, per altro verso, un *vademecum* tecnico che individua la tipologia di attività e le procedure che devono essere seguite nell'acquisizione e nell'analisi del dispositivo e dei dati[10].

Sotto il primo profilo, rileva, anzitutto, l'obbligo di indicare con precisione nel provvedimento di sequestro le informazioni che si intendono acquisire e la loro pertinenza rispetto all'ipotesi di reato. Qualora una simile operazione non fosse possibile[11], sorge il dovere di specificare le ragioni che giustificano un'apprensione onnicomprensiva del materiale informatico, essendo vietati sequestri con valenza meramente esplorativa[12]. Nel decreto devono poi essere illustrate le operazioni da effettuare sui dati e i criteri di selezione dei medesimi, nonché la durata temporale del vincolo.

Sotto il secondo profilo, la giurisprudenza richiede che nell'espletamento delle operazioni tecniche venga seguito uno specifico iter procedurale, che si compone di più passaggi[13]. Anzitutto, deve essere realizzata una copia forense del materiale informatico, e cioè una replica esatta (*bit* a *bit*) del contenuto del dispositivo[14]. Le analisi tecniche vengono poi effettuate su tale riproduzione, la quale, al termine delle operazioni, deve essere restituita al legittimo titolare[15].

2. Il controllo giurisdizionale preventivo: una garanzia di matrice europea e i (dis)orientamenti della giurisprudenza di legittimità.

In tale contesto, che, come si diceva, è contraddistinto da un progressivo rafforzamento delle garanzie che presidiano la procedura di acquisizione di dati digitali,

---

di pervenire al medesimo risultato. Su questi aspetti, v., per tutti, CAIANIELLO (2025b), pp. 1009 ss.

[9] In tal senso, tra le molte, v. Cass., sez. VI, 2 luglio 2019, n. 31593 e Cass., sez. VI, 24 ottobre 2019, n. 43556, nonché, da ultimo, Cass., Sez. VI, 10 febbraio 2026, n. 15409.

[10] Così PITTIRUTI (2021). Più di recente, la Cassazione ha affermato che tali regole non vanno considerate in maniera eccessivamente rigida, trattandosi piuttosto di criteri flessibili che devono essere diversamente calibrati a seconda delle circostanze del caso concreto: cfr. Cass, Sez. VI, 10 febbraio 2026, n. 133.

[11] «[I]n ragione della fase del procedimento, della fluidità delle indagini e della contestazione provvisoria, del fatto concreto per cui si procede, del tipo di illecito a cui il fatto sembra doversi ricondurre, della difficoltà di individuare nitidamente "ex ante" l'oggetto del sequestro, della natura del bene che si intende sequestrare»: in questi termini, v. Cass., Sez. VI, 22 settembre 2020, n. 34265.

[12] Quando, cioè, conducano ad un'«indiscriminata apprensione di una massa di dati informatici, senza alcuna previa selezione di essi e comunque senza l'indicazione degli eventuali criteri di selezione»: cfr. Cass., sez. VI, 17 aprile 2025, n. 24671. Da tempo la dottrina mette in guardia da un simile rischio: cfr. KOSTORIS (2011), p. 182.

[13] Cfr., in particolare, Cass., Sez. VI, 22 settembre 2020, n. 34265, par. 4.

[14] Sul concetto di copia forense, cfr. SIGNORATO (2024), pp. 157 ss.

[15] Senza che egli debba dimostrare uno specifico interesse a tal fine: cfr., ad es., Cass., Sez. II, 25 settembre 2025, n. 34324. Sul punto, per la verità, non vi è uniformità di vedute, dato che una parte della giurisprudenza ritiene che debba essere «dimostrata la sussistenza di un interesse concreto ed attuale alla disponibilità esclusiva dei dati contenuti nella copia estratta»: così Cass., Sez. II, 10 settembre 2024, n. 37409.

si innesta una recente pronuncia (*Bezirkshauptmannschaft Landeck*) della Grande Sezione della Corte di giustizia[16]. Quest'ultima era stata investita in via pregiudiziale da un tribunale austriaco affinché si pronunciasse sulla compatibilità delle regole interne relative all'accesso alle informazioni contenute in uno *smartphone* sottoposto a sequestro nell'ambito di un procedimento penale con il diritto europeo in materia di protezione dei dati personali[17]. Secondo il giudice rimettente, in base alla disciplina nazionale, l'acquisizione di tale materiale informatico potrebbe essere disposta direttamente dalla polizia giudiziaria, mentre le norme eurounitarie richiederebbero che una simile operazione debba essere subordinata ad un controllo giurisdizionale preventivo[18]. La Corte di giustizia aveva aderito a quest'ultima impostazione, ritenendo che la necessità di un vaglio *ex ante* fosse desumibile da una lettura congiunta della direttiva 2016/680/UE relativa alla protezione dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati (d'ora in poi "direttiva") e della Carta. In particolare, i giudici di Lussemburgo, nell'interpretare l'art. 4.1 lett. *c* direttiva, il quale prevede che «gli Stati membri dispongono che […] i dati personali siano adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono trattati», avevano stabilito che tale norma, in combinato disposto con gli artt. 7 e 8 Carta, andrebbe intesa nel senso che l'accesso al contenuto di uno *smartphone*, affinché non si traduca in un'ingerenza sproporzionata nella sfera privata dell'individuo (art. 52 Carta)[19], debba essere autorizzato da un giudice o da un'autorità amministrativa indipendente, poiché solo tali organi sarebbero «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].

La pronuncia della Corte di Giustizia è suscettibile di presentare un impatto dirompente nel nostro ordinamento, che, come noto, riconosce al p.m. e, nei casi d'urgenza, anche alla polizia giudiziaria, il potere di disporre il sequestro probatorio, confinando il controllo giurisdizionale su di esso ad una fase successiva all'emissione del provvedimento in seguito all'impugnazione del medesimo.

---

[16] C. Giust., *Bezirkshauptmannschaft Landeck*, C-548/21, 4 ottobre 2024.

[17] *Ibidem,* par. 20 ss.

[18] Domanda di pronuncia pregiudiziale proposta dal Landesverwaltungsgericht Tirol (Austria) il 6 settembre 2021 — C.G. / Bezirkshauptmannschaft Landeck, C-548/21.

[19] La Corte sembra operare una valutazione su due livelli, distinguendo tra una proporzionalità in astratto, al fine di stabilire se le regole austriache in materia di sequestro siano conformi al diritto europeo, e una proporzionalità in concreto, nella prospettiva di comprendere se vi è stata una corretta ponderazione dei valori in gioco nella specifica vicenda giudiziaria: cfr., al riguardo, MALACARNE (2025c), pp. 374 ss.

[20] C. Giust., *Bezirkshauptmannschaft Landeck*, cit., par. 103. Più flessibile appare, invece, l'approccio della Corte europea dei diritti dell'uomo, che, quando viene in gioco un atto lesivo delle garanzie individuali, non impone che esso sia subordinato all'autorizzazione del giudice, ma ritiene sufficiente la presenza di un controllo giurisdizionale anche a posteriori. Tale garanzia viene ricavata dalla clausola della "necessità in una società democratica" prevista dall'art. 8.2 Cedu: cfr., tra le molte, C. eur., *Roman Zakharov c. Russia*, 4 dicembre 2015, par. 257 ss. Sui diversi approcci delle due Corti europee, volendo BOLOGNARI (2026), *Judicial control over the EIO in the issuing State between mutual recognition and protection of human rights*.

Sollecitata a conformarsi a tale sentenza, la Cassazione ha assunto una posizione decisamente conservativa sul punto. Essa, infatti, pur con diverse accentuazioni, ha negato che il provvedimento ablativo debba essere autorizzato (o, comunque, immediatamente convalidato) dal giudice, adottando delle soluzioni interpretative che, pur tentando un 'dialogo' con la pronuncia della Corte di Giustizia, ne svuotano nella sostanza la portata precettiva.

In particolare, è possibile rinvenire tre orientamenti nella giurisprudenza di legittimità, che esprimono altrettante visioni del sistema di garanzie applicabili alla procedura di sequestro di dispositivi digitali.

3. La logica paternalistico-inquisitoria: il pm come autorità amministrativa indipendente.

In una prima sentenza[21], la Cassazione ha stabilito che la mancata previsione di un controllo giurisdizionale preventivo sul sequestro di dispositivi informatici non sarebbe incompatibile con il diritto europeo. Quest'ultimo, infatti, non prescriverebbe che il potere di autorizzare un simile provvedimento ablativo sia di esclusiva pertinenza del giudice, ma ammetterebbe che tale prerogativa possa essere esercitata anche da un'autorità amministrativa indipendente; autorità che, secondo la Corte di cassazione, coinciderebbe nel nostro ordinamento con il p.m., il quale «nell'esercizio delle sue funzioni pubbliche procede alle indagini secondo le specifiche regole dettate dal legislatore idonee a garantire anche i diritti dell'indagato»[22].

Una simile impostazione appare problematica sotto vari profili.

Anzitutto, la pronuncia in esame sembra eludere le indicazioni della Corte di giustizia. Infatti, quando quest'ultima richiede che l'acquisizione dei dati contenuti in un dispositivo possa essere autorizzata non solo da un giudice, ma anche da un'autorità amministrativa indipendente, non intenderebbe ricomprendere all'interno di questa categoria il p.m.[23]. Egli, essendo titolare dell'indagine e del potere di promuovere l'azione penale, non possiederebbe i necessari requisiti di terzietà e neutralità, che sono funzionali a garantire che il controllo preventivo sia condotto in modo obiettivo ed imparziale[24]. Una tale impostazione non è direttamente desumibile dalla sentenza *Bezirkshauptmannschaft Landeck*, che, del resto, si era pronunciata sulla conformità con la direttiva 2016/680/UE delle norme austriache che autorizzavano la polizia giudiziaria ad accedere ai dati contenuti in uno *smartphone*, ma si rinviene in un'altra importante decisione (*Prokuratuur*), a cui la prima, pur non rinviandovi in modo espresso, si

[21] Cass. pen., sez. V, 28 febbraio 2025, n. 8376.

[22] *Ibidem*, par 1.1.

[23] In tal senso, v. anche CAIANIELLO (2025), p. 1010.

[24] Così C. Giust., *Prokuratuur*, C-746/18, 2 marzo 2021, par. 53 ss., nonché, in senso analogo, C. Giust., *Commissioner of An Garda Síochána*, C-140/20, 5 aprile 2022, par. 109 e C. Giust., *La Quadrature du Net*, C-470/21, 30 aprile 2024, par. 126.

conforma implicitamente[25] e che, invece, riguardava la compatibilità tra la direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e il diritto estone, che consentiva al p.m. di acquisire i dati di traffico conservati dai fornitori di servizi di tali forme di comunicazione[26]. In base a quest'ultima pronuncia, che rappresenta un vero e proprio *leading case* in materia[27], non potrebbe essere attribuito all'organo inquirente il potere di effettuare il vaglio preventivo neppure nell'ipotesi in cui, come avveniva in Estonia, le regole nazionali gli conferiscano il potere di "verificare gli elementi a carico e quelli a discarico", di "garantire la legittimità del procedimento istruttorio" e di "agire unicamente in base alla legge ed al suo convincimento"[28].

Tali conclusioni, benché relative all'ordinamento estone, erano suscettibili di presentare ripercussioni significative anche nel nostro sistema processuale, dove il p.m., il quale presenta connotati assai simili a quelli individuati in tale sentenza[29], poteva acquisire, in base all'art. 132 d.lgs. 30 giugno 2003, n. 196 (c.d. codice della *privacy*), i dati di traffico telefonico e telematico conservati dai fornitori di servizi di telefonia ed internet senza un previo controllo giurisdizionale. Al fine di scongiurare il rischio che, in seguito alla proposizione di un'analoga questione pregiudiziale, la disciplina italiana venisse a sua volta dichiarata incompatibile con il diritto europeo[30], il nostro legislatore aveva modificato la norma in questione, stabilendo che l'acquisizione di tali dati dovesse essere subordinata all'autorizzazione del giudice[31].

Alla luce di tali rilievi, appare evidente come non sia sostenibile l'equiparazione tra p.m. ed autorità amministrativa indipendente prospettata dalla Corte di cassazione con riferimento al potere di disporre il sequestro di dispositivi digitali e l'acquisizione

---

[25] V., in particolare, C. Giust., *Bezirkshauptmannschaft Landeck*, cit., par. 102 ss., che, nell'individuare le caratteristiche che deve presentare il controllo preventivo, sostanzialmente parafrasa le espressioni impiegate in C. Giust., *Prokuratuur*, cit., par. 51 ss.

[26] In particolare, la Corte di giustizia era stata sollecitata a pronunciarsi in via pregiudiziale sull'interpretazione da attribuire all'art. 15.1 direttiva 2002/58/CE, che riconosce agli Stati il potere di adottare regole che limitino il diritto alla riservatezza delle comunicazioni e alla protezione dei dati personali in funzione della prevenzione e dell'accertamento dei reati. Secondo i giudici di Lussemburgo, tale previsione, letta congiuntamente agli artt. 7 e 8 Carta, andrebbe intesa nel senso che essa imporrebbe che l'accesso ai dati di traffico deve essere subordinato ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente.

[27] Sulla cui rilevanza nel nostro ordinamento molti si sono interrogati: cfr., tra gli altri e senza pretesa di completezza, ANDOLINA (2021), pp. 1204 ss.; CASCONE (2022), pp. 419 ss.; MALACARNE e TESSITORE (2022), pp. 1 ss.; MARCOLINI (2022), pp. 35 ss.

[28] C. Giust., *Prokuratuur*, cit., par. 56.

[29] Si pensi, ad esempio, alla norma che impone al p.m. di estendere l'attività investigativa anche a fatti e circostanze a favore dell'indagato (art. 358 c.p.p.), o alla previsione che gli riconosce il compito di vegliare alla osservanza delle leggi e alla pronta e regolare amministrazione della giustizia (art. 73 ord. giudiz.).

[30] All'epoca, similmente a quanto avviene oggi con riferimento al potere di disporre il sequestro, una parte della giurisprudenza interna aveva stabilito che l'acquisizione dei dati di traffico conservati dal gestore spettasse comunque al p.m. anche dopo la sentenza *Prokuratuur*: cfr., in particolare, Cass., sez. V, n. 33851 del 24 aprile 2018; Cass., sez. III, n. 36380 del 19 aprile 2019; nonché, in particolare, Cass., sez. III, n. 48737 del 25 settembre 2019.

[31] Su tale intervento normativo v. MALACARNE (2021).

dei dati in essi contenuti. Certo, si potrebbe obiettare che la sentenza *Prokuratuur* e la modifica normativa che ne è seguita riguardassero la diversa materia dell'accesso ai dati conservati dai *service provider*. Tuttavia, le affermazioni della Corte di giustizia relative ai connotati che devono contraddistinguere l'organo a cui è affidato il controllo preventivo sembrano presentare una portata più ampia, non solo perché, come si è osservato, la decisione *Bezirkshauptmannschaft Landeck* vi rinvia, seppur in modo implicito, ma anche per una ragione di fondo assai più pregnante, che riguarda i valori in gioco. Entrambe le pronunce, infatti, statuiscono che solo un vaglio preliminare effettuato da un organo terzo e neutrale possa garantire che l'invasione nella sfera privata dell'individuo determinata dall'acquisizione a fini investigativi di dati digitali non si traduca in una lesione sproporzionata del diritto alla riservatezza e alla protezione dei dati personali. Un simile controllo, come si è osservato, non potrebbe essere affidato al p.m.[32] neppure nell'ipotesi in cui, come avviene in Italia, egli non coltivi una prospettiva squisitamente persecutoria, ma si faccia carico di ricercare anche gli elementi a discarico (art. 358 c.p.p.)[33]. Tale prerogativa non va intesa nel senso che essa conferisce al titolare dell'accusa una posizione neutrale assimilabile a quella del giudice, ma integra in realtà una regola di prudenza, secondo la quale "l'indagante" che lavori "ad occhi chiusi", ignorando i materiali conoscitivi a favore della difesa, "rischia uno scacco al dibattimento o già all'udienza preliminare"[34].

Ritenere, invece, che il p.m., come sembra prospettare la Corte di cassazione, rappresenti una sorta di parte imparziale che esercita poteri analoghi a quelli del giudice allude ad una visione paternalistica tipica del processo di stampo inquisitorio, che non appare giustificabile in un sistema accusatorio come il nostro[35].

4. La logica compensativa: il tentativo di controbilanciare l'assenza di un controllo giurisdizionale *ex ante* con la possibilità di esperire il rimedio del riesame.

Di segno diverso appare, invece, una seconda sentenza della Suprema Corte[36]. Discostandosi esplicitamente dall'orientamento sul quale ci si è soffermati poc'anzi, la pronuncia sembra conformarsi alle indicazioni provenienti dalla Corte di Giustizia, affermando che il sequestro debba essere assoggettato ad un controllo giurisdizionale di tipo autorizzatorio, quando sia funzionale all'accesso dei dati contenuti in un dispositivo digitale. Per questo motivo, allo stato, la normativa interna non apparirebbe conforme

---

[32] V. però, NICOLINI (2026), il quale ritiene, invece, che una simile prerogativa appartenga al p.m., purché egli "eserciti la propria funzione con piena responsabilità e senso istituzionale, impegnandosi nella motivazione dei propri provvedimenti a rendere ragione del percorso logico-giuridico che li sorregge e delle esigenze investigative che intende perseguire in vista della piena realizzazione del principio di obbligatorietà dell'azione penale".

[33] Come evidenziato anche da LASAGNI (2018), p. 397.

[34] Così CORDERO (2012), p. 815.

[35] Cfr. FERRUA (1997), p. 44.

[36] Cass. pen., sez. VI, 1 aprile 2025, n. 13585. Per un commento a prima lettura di questa pronuncia, v. MALACARNE (2025a).

al diritto europeo, il quale esclude che un simile vaglio possa essere effettuato dal p.m., che non rappresenterebbe un organo terzo, ma una parte processuale[37].

Tuttavia, nonostante questa presa di posizione, la Cassazione considera che, pur mancando nel caso di specie un controllo giurisdizionale *ex ante*, non risulterebbero in concreto pregiudicate le garanzie difensive della persona destinataria del sequestro, poiché il nostro sistema ammette che un simile provvedimento sia comunque impugnabile attraverso il riesame, il quale non solo «impone una decisione in tempi strettissimi», ma implica altresì che il giudice effettui un vaglio di legittimità e di merito sulla «correttezza del provvedimento, la congruità e la comparazione degli interessi in gioco», consentendo «un esame effettivo e indipendente circa la necessità, proporzionalità e minimizzazione dell'acquisizione dei dati»[38].

Tale impostazione palesa una certa contraddittorietà. La sentenza, infatti, per un verso, stabilisce che il controllo giurisdizionale preventivo sul sequestro integra un presupposto indefettibile, precisando che un simile vaglio, come richiesto dalla Corte di giustizia[39], debba intervenire prima di qualsiasi tentativo di accesso ai medesimi, mentre, dall'altro, nega questo assunto, ritenendo che in concreto tale lacuna non sarebbe lesiva delle garanzie difensive, le quali sarebbero pienamente tutelate dalla possibilità di proporre il riesame[40]. E non varrebbe obiettare che la sentenza *Bezirkshauptmannschaft Landeck* ammette che, «in casi d'urgenza debitamente comprovati», sarebbe possibile un controllo successivo, purché avvenga in tempi brevi (par. 104). Va, infatti, precisato che in questo passaggio la Corte di Giustizia non sembrerebbe alludere tanto ad un vaglio attivabile attraverso l'impugnazione del provvedimento ablativo, quanto piuttosto alla procedura di convalida. Se i giudici di Lussemburgo avessero ritenuto che il controllo successivo avrebbe potuto assumere anche le caratteristiche di un gravame, è ipotizzabile che non sarebbe stata accolta la questione pregiudiziale sollevata dal tribunale austriaco: infatti, in base al diritto di quel Paese, è possibile proporre un ricorso (*Beschwerde*) contro qualsiasi misura investigativa (compreso il sequestro di dispositivi e dati digitali) davanti ad un giudice (*Beschwerdegericht*), che ha il potere di operare un vaglio di legittimità e di merito del provvedimento (§§87-88 StPO)[41].

In ogni caso, anche volendo ammettere che sia possibile attribuire un significato più ampio alla nozione di controllo *ex post* a cui allude la Corte di Giustizia, ricomprendendovi pure il riesame, va evidenziato che la Cassazione non circoscrive l'esperibilità di un simile mezzo di impugnazione ai casi eccezionali di necessità e di urgenza, come richiesto dalla sentenza *Bezirkshauptmannschaft Landeck*, ma afferma che

---

[37] Cass. pen., sez. VI, 1 aprile 2025, n. 13585, par. 5.

[38] *Ibidem*, par. 6, nonché, in senso analogo, Cass. pen., sez. II, 29 gennaio 2026, n. 3765 e, con riferimento al sequestro disposto d'urgenza dalla pp.g., Cass. pen., sez. III, 18 novembre 2025, n. 2218, par. 2.1, con commento di GIORDANO (2026).

[39] C. Giust., *Bezirkshauptmannschaft Landeck*, cit., par. 104.

[40] Ritiene, invece, condivisibile un simile approccio PALMA (2026), pp. 2115 ss.

[41] In Austria è previsto, inoltre, uno specifico mezzo di impugnazione (*Einspruch*) contro le misure investigative che ledano i diritti fondamentali (§106 StPO). Esso può essere esperito in via autonoma, ma, ove venga parallelamente presentato anche un ricorso ai sensi dei §§87-88 StPO, il codice di rito ne impone la proposizione congiunta (§106.2 StPO).

esso integra lo strumento ordinario attraverso il quale contestare la legittimità del provvedimento ablativo.

Appare poi censurabile sotto il profilo dogmatico l'equiparazione che la Corte di cassazione prospetta tra le due tipologie di controllo. Esse, infatti, assolvono funzioni diverse. Pur essendo innegabile che il vaglio *ex post* effettuato con il riesame, oltre a vertere sui presupposti del provvedimento impugnato, riguardi anche le modalità con le quali si è svolto il sequestro e, quindi, per sua natura, presenti una portata più ampia, solo una verifica operata *ex ante* dal giudice, intervenendo prima che si svolgano le operazioni acquisitive, impedirebbe fin dall'inizio che l'accesso ai dati si traducesse in una compressione dei diritti fondamentali[42]. Non va poi dimenticato che, subordinando il controllo giurisdizionale all'iniziativa di parte attraverso l'impugnazione del provvedimento ablativo, ne viene di molto depotenziata la portata.

Inoltre, ragionando in questo modo la Corte di cassazione, sembra applicare, seppur in modo implicito, la logica compensativa che contraddistingue la giurisprudenza della Corte europea dei diritti dell'uomo in materia di garanzie processuali. In base a tale approccio, una violazione dei diritti consacrati dalla Cedu sarebbe tollerabile in presenza di altri fattori che consentano di controbilanciarne gli effetti negativi (c.d. *as a whole test*)[43]. Si tratta evidentemente di un'impostazione regressiva[44] che, lungi dal rafforzare le garanzie, ne determina in realtà uno svilimento: considerare che la mancanza di un controllo giurisdizionale *ex ante* possa essere compensata da un vaglio *ex post* comporta, infatti, un impoverimento dell'apparato di tutela posto a presidio della persona destinataria del sequestro, la quale, potendo beneficiare del solo mezzo del riesame, sarebbe esposta al rischio di un accesso indiscriminato ai propri dati[45].

---

[42] In un'analoga prospettiva, seppur con riferimento all'acquisizione transnazionale di messaggi scambiati all'interno di una piattaforma criptata, cfr. DANIELE (2025), pp. 3-4. Sul presupposto che il vaglio *ex post* non assicuri una tutela sufficiente ai valori in gioco, la dottrina italiana avverte da tempo l'esigenza di predisporre un controllo giurisdizionale di tipo autorizzatorio sul sequestro di dispositivi digitali: cfr., *ex multis*, CHELO (2022), pp. 1588 ss.; CURTOTTI (2024), p. 2703; DINACCI (2025); FILIPPI (2024); LASAGNI (2018), pp. 395 ss.; MALACARNE (2025a); MALACARNE (2025b), pp. 131 ss.; MURRO (2024a), pp. 253 ss.

[43] Emblematico in tal senso quanto affermato dalla Grande camera della Corte europea nella nota sentenza *Al Khawaya e Thaery c. Regno unito*, 15 dicembre 2011, la quale, pur ravvisando la violazione del diritto dell'imputato a non essere condannato sulla base unica o determinante di dichiarazioni rese da testi che egli non abbia mai avuto occasione di esaminare, ha ritenuto che la compressione di una simile garanzia debba comunque ritenersi in concreto controbilanciata da una serie di 'vantaggi' di cui avrebbe beneficiato l'imputato, come la possibilità di fornire comunque la sua versione dei fatti e di contestare la credibilità del teste assente e la coerenza delle sue affermazioni, evidenziandone il contrasto con le dichiarazioni di altri dichiaranti.

[44] In generale, in una prospettiva critica rispetto all'approccio compensativo adottato dalla Corte europea, cfr. CAIANIELLO (2017), pp. 283 ss. e KOSTORIS (2020a), pp. 1675 ss., nonché, anche con riferimento alle ricadute che una simile impostazione presenta sulla giurisprudenza interna, BOLDRIN (2021), pp. 1 ss.

[45] Non si tratta, invero, di una novità nel panorama giurisprudenziale interno. Particolarmente significativa in tal senso appare la nota sentenza n. 132 del 2019 della Corte costituzionale, che, richiamando il *case law* della Corte europea, ha invitato il legislatore a introdurre "ragionevoli eccezioni al principio dell'identità tra giudice avanti al quale è assunta la prova e giudice che decide, in funzione dell'esigenza, costituzionalmente rilevante, di salvaguardare l'efficienza dell'amministrazione della giustizia penale, in

5. La logica 'riduttiva': l'applicazione del previo controllo giurisdizionale al solo accesso ai dati.

È infine possibile identificare un terzo orientamento nell'ambito della giurisprudenza di legittimità. Esso appare improntato ad una logica che si potrebbe definire 'riduttiva'[46]. In particolare, la suprema Corte circoscrive la portata della sentenza della Corte di giustizia, operando una distinzione tra l'acquisizione del dispositivo e dei dati in esso contenuti, che non richiederebbe l'autorizzazione da parte del giudice, e l'accesso a tali dati, che invece lo imporrebbe. Dunque, nell'ipotesi in cui il sequestro del *device* e dei dati sia stato disposto dal p.m., non vi sarebbe incompatibilità tra il diritto interno e l'art. 4.1 lett. *c* direttiva 2016/680/UE, che comunque non potrebbe essere applicato direttamente dal giudice nazionale, poiché si limiterebbe ad esprimere «indirizzi rivolti al legislatore»[47]. In ogni caso, secondo la Corte, le operazioni eseguite sul dispositivo sarebbero conformi alle indicazioni contenute nella sentenza *Bezirkshauptmannschaft Landeck* se, come avvenuto nel caso sottoposto all'attenzione dei giudici di legittimità, l'accesso al materiale informatico avvenisse in sede di incedente probatorio e, quindi, davanti ad un giudice nel contraddittorio delle parti.

Non si tratta di un orientamento isolato. Nel medesimo solco tracciato dalla sentenza che si è esaminata sembra, infatti, collocarsi una seconda pronuncia, la quale, dopo aver ribadito che alla direttiva non potrebbe essere riconosciuta efficacia diretta, afferma che le garanzie previste dal diritto europeo sarebbero pienamente tutelate anche ove l'acquisizione del dispositivo e dei dati sia stata disposta dal p.m., ma l'analisi del materiale informatico sia avvenuta nell'ambito di un accertamento tecnico non ripetibile (art. 360 c.p.p.)[48]. Infatti, secondo la Corte, tale procedura assicurerebbe, per un verso, che le operazioni siano affidate ad un "soggetto diverso dalla polizia giudiziaria e dal pubblico ministero" e, per altro verso, che l'indagato possa nominare un difensore e un proprio consulente affinché assistano al conferimento dell'incarico, partecipino all'accertamento e formulino osservazioni, essendogli anche riconosciuto il potere di promuovere una riserva di incedente probatorio[49].

Tralasciando per ora il delicato profilo dell'efficacia nel nostro ordinamento della norma contenuta nella direttiva 2016/680/UE, sul quale ci si soffermerà più avanti[50], sembra doversi respingere anche questa impostazione.

---

presenza di meccanismi "compensativi" funzionali all'altrettanto essenziale obiettivo della correttezza della decisione", come, ad esempio, la videoregistrazione delle prove dichiarative (par. 3.2). Numerose naturalmente le voci critiche che si sono levate contro questa sentenza: cfr., *ex multis*, DANIELE (2021), pp. 53 ss.; FERRUA (2020), pp. 7 ss.; MAZZA (2019), pp. 1 ss.

[46] Cass. pen., sez. VI, 4 aprile 2025, n. 17686.

[47] *Ibidem*, par. 5.

[48] Cass., Sez. II, 13 novembre 2025, n. 40451, par. 2.8 ss.

[49] *Ibidem*, par. 2.9.2.

[50] V. *infra* par. 5 *b*

Il legislatore europeo attribuisce alla nozione di trattamento dei dati personali un significato assai ampio, ricomprendendovi ogni operazione compiuta su tale tipologia di dati, come "la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione" (art. 3 direttiva). Si tratta di un'elencazione non tassativa[51], all'interno della quale ben potrebbe essere inserita anche l'acquisizione di un dispositivo digitale e del materiale informatico in esso contenuto, che in tal modo entra nella disponibilità dell'autorità giudiziaria[52].

In ogni caso, anche volendo ritenere che l'apprensione del *device* non integri un "trattamento" nel senso attribuito a questa espressione dalla direttiva, non sarebbe condivisibile la tesi – sostenuta dalla Cassazione – in base alla quale l'accesso al materiale informatico in sede di incidente probatorio o di accertamento tecnico non ripetibile garantirebbe, di per sé, "il rispetto dei parametri indicati dalla Corte di giustizia"[53]. Quest'ultima, come si è osservato[54], richiede che il controllo del giudice intervenga prima di ogni tentativo di intrusione nel dispositivo, sul presupposto che tale operazione è suscettibile di disvelare una mole significativa di informazioni[55], che consentono di «trarre conclusioni molto precise riguardo alla vita privata della persona interessata»[56] e che, in buona parte, sono prive di rilevanza investigativa. Solo un vaglio preventivo scongiurerebbe il rischio che l'estrazione del materiale informatico si traduca in una violazione delle garanzie individuali e, in particolare, del diritto alla riservatezza (art. 7 Carta) e di quello alla protezione dei dati personali (art. 8 Carta).

Dal canto loro, l'accertamento tecnico non ripetibile e l'incidente probatorio non offrono una tutela anticipata, ma solo successiva, limitandosi ad assicurare un contraddittorio limitato alle operazioni tecniche.

Particolarmente criticabile appare poi il rilievo in base al quale il consulente tecnico del p.m. integrerebbe un soggetto diverso rispetto al p.m. e alla p.g.[57]. Una simile affermazione pare alludere al fatto che l'esperto nominato dall'accusa rappresenti un organo terzo. Pur non pronunciandosi espressamente sul punto, la Cassazione sembra, però, implicitamente aderire a questa impostazione, quando evidenzia che per la Corte

---

[51] C. Giust., *Bezirkshauptmannschaft Landeck*, cit., par. 72.

[52] Per un'interpretazione estensiva del concetto di "trattamento" v. anche C. Giust., *Bezirkshauptmannschaft Landeck*, cit., par. 75, secondo la quale rientrerebbe in tale nozione non solo l'accesso ai dati, ma anche il tentativo di visualizzare i medesimi, sul presupposto che altrimenti si esporrebbero le persone coinvolte a un rischio significativo che una violazione dei diritti previsti dalla direttiva non possa più essere evitata.

[53] Cass. pen., sez. VI, 4 aprile 2025, n. 17686, par. 5., nonché, in un'analoga prospettiva, Cass., Sez. II, 13 novembre 2025, n. 40451, par. 2.9 ss.

[54] V. *supra* par. 3.

[55] «[…] non soltanto dati relativi al traffico e alla localizzazione, ma anche fotografie e la cronologia di navigazione su Internet effettuata con tale telefono, o addirittura una parte del contenuto delle comunicazioni effettuate con detto telefono, in particolare consultando i messaggi che vi sono conservati»: cfr. C. Giust., *Bezirkshauptmannschaft Landeck*, cit., par. 92.

[56] *Ibidem*, par. 93.

[57] Cass., Sez. II, 13 novembre 2025, n. 40451, par. 2.9.2.

di giustizia non rileverebbe tanto la qualifica formale dell'organo che effettua il controllo preventivo, il quale potrebbe coincidere sia con il giudice sia con l'autorità amministrativa indipendente, quanto piuttosto la sua terzietà[58]. Tuttavia, proprio questa caratteristica non potrebbe essere attribuita al consulente tecnico del p.m.: egli rappresenta un ausiliario dell'accusa, anche in un contesto in cui viene formata la prova. Attribuendo un simile connotato al consulente tecnico, la cassazione sembra far rivivere – e, addirittura, enfatizzare – quelle ambiguità che caratterizzavano il vecchio rito sommario, dove però le operazioni tecniche erano affidate ad un perito, che, pur nominato dal p.m., aveva l'obbligo di "far conoscere la verità" e poteva essere ricusato[59].

Una simile impostazione sembra poi ridare slancio a quella censurabile – e, sino ad oggi, isolata – giurisprudenza che attribuisce una «sostanziale priorità» alle conclusioni a cui giunge l'ausiliario scientifico dell'accusa «rispetto a quelle tratte dalla consulenza tecnica della difesa»[60]. Secondo la Cassazione, andrebbe attribuita una fede privilegiata alle indagini del p.m. sul presupposto che quest'ultimo avrebbe la funzione di accertare la verità e di ricercare anche le prove a discarico ai sensi dell'art. 358 c.p.p. Viene così effettuata una perniciosa assimilazione tra organo inquirente e giudice, anche qui secondo una logica tipica del processo inquisitorio[61].

Ciò appare ancor più sorprendente se si considera che la Cassazione, in un passaggio che precede di poche righe l'affermazione relativa alla terzietà del consulente dell'accusa, si è esplicitamente discostata[62] da quel precedente in base al quale il p.m. integrerebbe un organo amministrativo indipendente[63]. Sotto questo profilo, la sentenza giunge all'esito paradossale di prendere formalmente le distanze da una propria pronuncia, ma nella sostanza di conformarvisi.

Vanno, infine, fatte alcune precisazioni con riferimento alle garanzie partecipative, che la Cassazione valorizza nella prospettiva di affermare che l'accesso ai dati nell'ambito di un accertamento tecnico non ripetibile o di un incidente probatorio assicura il pieno rispetto delle garanzie individuali stabilite dal diritto europeo. A tal fine, occorre distinguere a seconda che il contraddittorio abbia riguardato esclusivamente la creazione della copia dei dati o sia stato esteso anche alla loro selezione. La sola partecipazione alla realizzazione del duplicato, pur assicurando, in linea di principio, la correttezza di tale operazione, non sarebbe suscettibile di impedire che l'accesso al contenuto del dispositivo, essendo effettuato in autonomia dall'autorità giudiziaria, ecceda i limiti dello stretto necessario, come paventato dalla Corte di giustizia.

---

[58] *Ibidem*, par. 2.7.5.

[59] Cfr. KOSTORIS (1993), p. 149.

[60] Cass., Sez. III, 18 febbraio 2020, n. 16458, pp. 4.

[61] In tal senso, KOSTORIS (2020b).

[62] Cfr. Cass., Sez. II, 13 novembre 2025, n. 40451, par. 2.7.6: "[…] non è condivisibile la pronuncia di questa Corte che ha ritenuto che la normativa nazionale non ponga problemi di compatibilità con il diritto dell'Unione europea in quanto al pubblico ministero può essere riconosciuta, nel nostro sistema processuale, la natura di «organo amministrativo indipendente»".

[63] V. *supra* par. 2.

Minori criticità si profilerebbero, invece, nell'ipotesi in cui la difesa abbia avuto la possibilità di interloquire anche sul processo selettivo. In questo caso, che, beninteso, non coincide sotto il profilo formale con una previa autorizzazione da parte del giudice, la quale, come si diceva, offre comunque una tutela più forte, il conflitto con la giurisprudenza europea sarebbe meno marcato, poiché la difesa potrebbe presentare, anche tramite un proprio consulente, proposte e rilievi funzionali a garantire che l'accesso ai dati non si traduca in un'invasione sproporzionata nella sfera individuale, assicurando al contempo una maggiore trasparenza investigativa e un miglior accertamento dei fatti[64].

6. Le conseguenze processuali della mancata previsione di un controllo giurisdizionale *ex ante*.

Una volta delineate le varie posizioni espresse dalla giurisprudenza di legittimità, occorre domandarsi quali conseguenze processuali siano ipotizzabili in caso di inosservanza di una norma europea che prescrive la necessità di un previo controllo giurisdizionale sull'atto di acquisizione dei dati contenuti in un dispositivo elettronico. Occorre cioè chiarire se in un caso del genere sia possibile riscontrare una forma di invalidità del provvedimento ablativo, o se, invece, debbano essere prospettate soluzioni alternative.

Per rispondere ad un simile quesito, occorre preliminarmente cercare di chiarire quale efficacia assuma nel nostro ordinamento l'art. 4.1 lett. *c* direttiva, nell'interpretazione che ne dà la Corte di giustizia.

Come noto, le direttive presentano di regola efficacia indiretta, essendo vincolanti quanto al risultato da raggiungere (art. 288 TFUE). La scelta dei mezzi e delle forme con i quali darvi attuazione è, invece, lasciata agli Stati. Tuttavia, qualora sia decorso il termine entro il quale recepire simili atti normativi, o sia stata data loro parziale o insufficiente attuazione, può essere riconosciuta ai medesimi efficacia diretta, purché essi contengano norme chiare, precise e incondizionate[65].

La direttiva 2016/680/UE è stata recepita in Italia entro il termine di attuazione fissato dalla medesima con d. lgs. 18 maggio 2018, n. 51. Quest'ultimo non contempla che l'accesso ai dati contenuti in un dispositivo digitale debba essere subordinato all'autorizzazione da parte del giudice. Tuttavia, una simile lacuna non sarebbe attribuibile ad una condotta inadempiente da parte del nostro Paese, dato che, all'epoca in cui è stata implementata la direttiva, non era possibile desumere dal testo di tale atto la necessità di un controllo giurisdizionale *ex ante*, il quale, come si è evidenziato, è stato ricavato successivamente in via interpretativa dalla Corte di giustizia da una norma che

[64] In una simile prospettiva, con riferimento al d.d.l. S.806, che mira ad introdurre nel codice di rito una specifica ipotesi di sequestro di dispositivi, sistemi informatici o telematici o memorie digitali, cfr. CAIANIELLO (2025a).

[65] Cfr. KOSTORIS (2025), p. 25.

si limitava ad invitare gli Stati membri a disporre che i dati personali siano adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono trattati (art. 4.1 *c*).

Il carattere 'programmatico' di tale previsione sconsiglierebbe di riconoscere ad essa efficacia diretta. Eppure, è innegabile che, per effetto della sentenza *Bezirkshauptmannschaft Landeck*, la norma presenti una diversa fisionomia, assumendo confini più definiti, che indurrebbero a ritenere che essa possa, invece, avere natura *self-executing* nel nostro ordinamento. Naturalmente, ad una simile conclusione si potrebbe giungere solo a patto di riconoscere alle pronunce che risolvono una questione pregiudiziale valore cogente *erga omnes*. Si tratta di una tesi che non sembra trovare specifici ancoraggi sul piano normativo[66], ma che la Corte di giustizia, nella prospettiva di assicurare l'unità del sistema comunitario, ha ricavato dalla regola in base alla quale l'obbligo di proporre il rinvio pregiudiziale verrebbe meno ove essa si sia già pronunciata sulla medesima questione[67].

Alla luce di un quadro così complesso, è inevitabile che determinare se nel caso di specie l'art. 4.1 lett. *c* direttiva presenti o meno efficacia diretta nel nostro ordinamento non risulti affatto un'operazione agevole, come del resto pare confermato anche dalle diverse posizioni assunte dalla Corte di cassazione sul punto.

Le prime due pronunce sembrano postulare, benché manchi una statuizione esplicita sul punto, la diretta applicabilità nel nostro ordinamento di tale previsione, negando però, come si è detto, che il sequestro debba essere necessariamente autorizzato, o comunque convalidato, dal giudice[68].

Dal canto loro, le ultime due sentenze della Cassazione che si sono esaminate negano in radice la natura *self-executing* dell'art. 4.1 lett. *c* Direttiva, affermando che tale previsione si limiterebbe a fornire delle indicazioni al legislatore[69].

Conviene soffermarsi su entrambe le prospettive, anticipando sin d'ora come si ritenga preferibile la seconda, che promuove l'efficacia solo indiretta della norma eurounitaria. Quest'ultima, come si diceva, appare formulata in termini estremamente generici, esprimendo non tanto delle prescrizioni specifiche, quanto piuttosto delle opzioni valoriali rivolte agli Stati, che sono chiamati ad assicurare l'adeguatezza, la pertinenza e la non eccedenza dei dati rispetto alle finalità per i quali essi sono trattati.

a. Le implicazioni del riconoscimento di un'efficacia* self-executing *all'art. 4.1 lett. c direttiva 2016/680/UE. Qualora si ritenga che la previsione contenuta nell'art. 4.1 lett. *c* nell'interpretazione che ne dà la Corte di giustizia presenti efficacia diretta, occorre domandarsi se il sequestro compiuto in violazione della medesima debba essere

---

[66] Non si potrebbe far leva a tal fine sull'art. 19 TUE, il quale assegna alla Corte di giustizia il compito di assicurare il rispetto del diritto nell'interpretazione e nell'applicazione dei trattati. In realtà, tale norma non sembra tanto conferire portata generale al *case law* della Corte di giustizia, quanto piuttosto attribuire alla medesima una funzione nomofilattica, simile a quella che contraddistingue la nostra Corte di cassazione: così KOSTORIS (2025), p. 37.

[67] A partire, in particolare, dalla nota sentenza C. giust., *Da Costa*, C-28-30/62, 7 marzo 1963.

[68] Cass. pen., sez. V, 28 febbraio 2025, n. 8376, par. 1.1 e Cass. pen., sez. VI, 1 aprile 2025, n. 13585, par. 6.

[69] Cass. pen., sez. VI, 4 aprile 2025, n. 17686, par. 5, nonché, più di recente, Cass., Sez. II, 13 novembre 2025, n. 40451, par. 2.8 ss.

considerato invalido. Nell'ipotesi in cui si dia risposta positiva al quesito, è necessario chiarire se l'inosservanza della norma eurounitaria implichi la nullità del provvedimento ablativo, o se, invece, in una situazione del genere sia possibile diagnosticare l'inutilizzabilità del materiale probatorio acquisito.

Mentre la prima sentenza che si è esaminata risolve la questione affermando la piena compatibilità del quadro normativo attuale con il diritto europeo, sul presupposto – non condivisibile, per le ragioni che si sono illustrate – che il p.m., rappresentando un'autorità amministrativa indipendente, potrebbe direttamente disporre il sequestro, la seconda pronuncia adotta, invece, come si è visto, un approccio più problematico. Anzitutto, la Cassazione nega che sia possibile ricavare divieti probatori dal diritto europeo. A supporto di questa affermazione, viene riportato un passaggio di una nota sentenza della Corte di giustizia, in base al quale «spetta, in linea di principio, unicamente al diritto nazionale determinare le norme relative all'ammissibilità e alla valutazione, nell'ambito di un procedimento penale, di informazioni e di elementi di prova che sono stati ottenuti con modalità contrarie al diritto dell'Unione»[70]. Poiché nel nostro ordinamento mancherebbe una norma che prevede l'inutilizzabilità della prova acquisita mediante un sequestro informatico disposto dall'organo inquirente anziché dal giudice, non potrebbe ricorrere nel caso di specie questa forma di invalidità. Una simile affermazione sembra condivisibile[71]: in effetti, né la normativa di recepimento della direttiva, né tantomeno il codice, che, come noto, addirittura autorizza il p.m. (e, in taluni casi, anche la p.g.) a disporre il provvedimento ablativo, prevedono uno specifico divieto probatorio che sanzioni l'inosservanza di una norma europea che prescriva la necessità di un previo controllo giurisdizionale sul sequestro di dati digitali[72].

La Cassazione, a questo punto, si domanda se in un caso del genere sia prospettabile, invece, la nullità del provvedimento ablativo. A tal fine, la sentenza rinvia nuovamente alla giurisprudenza della Corte di giustizia, la quale afferma che sul giudice nazionale incombe il dovere «di espungere (*disregard*), nell'ambito di un procedimento penale avviato a carico di una persona sospettata di atti di criminalità, informazioni ed elementi di prova se tale persona non è in grado di svolgere efficacemente le proprie osservazioni su tali informazioni ed elementi di prova»[73]. Secondo la Suprema Corte, l'inosservanza della norma che prescrive un controllo di tipo autorizzatorio del giudice sul sequestro sarebbe suscettibile di condurre alla nullità del provvedimento ablativo, in

---

[70] C. Giust., *M.N.*, C-670/22, 20 aprile 2024, par. 128. Si tratta, per la verità, di un orientamento consolidato della Corte, che ha ribadito in più occasioni tale statuizione. Si veda, ad es., C. Giust., *La Quadrature du Net e a.*, C-511/18, C-512/18 e C-520/18, 6 ottobre 2020, par. 222, a cui la prima sentenza espressamente rinvia, ma un'affermazione analoga compare pure in C. Giust., *Prokuratuur*, cit., par. 41.

[71] Anche se non manca chi sostiene che la trasgressione della norma eurounitaria dovrebbe condurre, invece, all'inutilizzabilità del materiale probatorio: cfr. CAMON (2025b), p. 421.

[72] In tal senso, v. anche SCHIAVONE (2026), p. 166, nonché, sia pur con riferimento alla diversa ipotesi di acquisizione transfrontaliera di comunicazioni raccolte all'estero, DANIELE (2023).

[73] C. Giust., *M.N.*, cit., par. 131, nonché, analogamente, C. Giust., *Prokuratuur*, cit., par. 44. Sulla *ratio* di tale regola, v. PANZAVOLTA e MAES (2022), pp. 199 ss.

considerazione del fatto che esso sarebbe stato disposto in violazione delle garanzie difensive da un organo (il p.m.) che difetterebbe di un simile potere[74].

Pur non esprimendosi in modo chiaro sul punto, la Suprema Corte sembrerebbe propendere per un'inclusione di tale invalidità all'interno dell'art. 178 co. 1 lett. *c* c.p.p.: il controllo giurisdizionale *ex ante* costituirebbe, dunque, un presidio fondamentale nella prospettiva di consentire l'esercizio delle prerogative difensive[75]. Ne consegue che, solo evitando un accesso indiscriminato ai dati attraverso il previo vaglio del giudice sulla misura investigativa, si assicura la piena protezione del diritto di difesa. Si viene così a realizzare un inedito collegamento tra tale garanzia e la *privacy*: la protezione della seconda rappresenta, infatti, il presupposto necessario per l'espletamento della prima.

Tuttavia, la Cassazione, pur affermando che sia possibile in astratto far discendere dall'inosservanza del diritto europeo la nullità del sequestro, rinuncia a dichiararla nel caso di specie, sul presupposto che una simile sanzione potrebbe giustificarsi solo ove venisse negata al destinatario del sequestro la «concreta possibilità di difendersi»[76]. Poiché, invece, gli è riconosciuto il potere impugnare il provvedimento ablativo con il riesame, che, come si è detto, consente di attivare in tempi brevi un controllo di legittimità e di merito sulla correttezza e congruità del sequestro, non si verificherebbe una violazione delle garanzie difensive.

Tale impostazione sembra alludere ad una visione del processo che presenta una forte impronta 'europea'[77], dove gioca un ruolo centrale il concetto di pregiudizio effettivo[78]. In questa prospettiva, al fine di diagnosticare un'invalidità non conterebbe tanto la difformità dell'atto al modello legale, secondo la logica formale imperniata sui principi di legalità e tassatività che contraddistingue il nostro ordinamento[79], quanto piuttosto l'impatto che una simile trasgressione determina in una specifica vicenda giudiziaria[80]. Secondo questo schema, basato su un approccio antiformalistico e sostanziale, un'invalidità potrebbe essere dichiarata solo ove l'atto sia concretamente offensivo per i valori in gioco [81].

---

[74] Cass. pen., sez. VI, 1 aprile 2025, n. 13585, par. 6.

[75] Secondo SCHIAVONE (2026), pp. 168 ss., il sequestro dei dati disposto dal p.m. dovrebbe essere considerato invalido, in quanto tale organo sarebbe privo della necessaria competenza funzionale per emettere il provvedimento; circostanza quest'ultima che andrebbe equiparata, quanto al regime, ad una nullità assoluta, essendo insanabile e rilevabile d'ufficio in ogni stato e grado del procedimento.

[76] Cass. pen., sez. VI, 1 aprile 2025, n. 13585, par. 6.

[77] Fenomeno che, per effetto della pervasività del diritto europeo nel campo della giustizia penale, si sta affermando in maniera sempre crescente nel nostro ordinamento: cfr., tra i molti, CERESA GASTALDO e LONATI (2021); CAIANIELLO e MANES (2020); DONINI (2011); KOSTORIS (2025).

[78] Come evidenziato, in particolare, da CAIANIELLO (2012), pp. 135 ss. e da PAULESU (2014), pp. 882 ss.

[79] Su tale logica, cfr., tra i molti e senza pretesa di completezza, CONSO (1955), pp. 307 ss.; CORDERO (1961), pp. 680 ss.; GALANTINI (1999), pp. 340 ss.; RAFARACI (1998), pp. 597 ss.

[80] Sulla difficile convivenza tra questi paradigmi v. CAIANIELLO (2012), pp. 9 ss., nonché APRATI (2018), pp. 16 ss.

[81] CAIANIELLO (2012), pp. 131 ss., nonché PAULESU (2023), p. 296, secondo il quale «valorizzare il criterio del pregiudizio effettivo significa guardare oltre le forme. Significa cioè riconoscere al giudice il potere di verificare di volta in volta la concreta offensività dell'atto imperfetto».

Tuttavia, le conclusioni a cui giunge la Cassazione non appaiono coerenti rispetto alle premesse metodologiche da cui muove la pronuncia in esame.

Una volta stabilito che l'art. 4.1 lett. *c* Direttiva presenta efficacia *self-executing* nel nostro ordinamento e che il controllo preventivo da parte del giudice costituisce un requisito di validità del sequestro, non si potrebbe sostenere che la mancanza di un tale vaglio, essendo 'controbilanciata' dalla possibilità di impugnare il provvedimento ablativo con il riesame, integri un vizio innocuo e che, dunque, non sia riscontrabile in tal caso un pregiudizio effettivo. Un simile criterio appare, infatti, privo di una base normativa, ponendosi in contrasto con il principio di legalità processuale[82].

Né si potrebbe ritenere che una situazione del genere sia inquadrabile all'interno della fattispecie regolata dall'art. 183 co. 1 lett. *b* c.p.p.[83], sul presupposto che la possibilità di esperire il riesame, assicurando il conseguimento dello scopo a cui è preordinato l'atto invalido, produrrebbe un effetto sanante della nullità dovuta alla mancata previsione di un vaglio *ex ante*. Come si è osservato in più occasioni, le due forme di controllo non possono essere ritenute equivalenti, poiché assolvono a funzioni diverse. Se la Cassazione considera che l'autorizzazione del giudice sia indispensabile al fine di assicurare la protezione delle garanzie difensive, la conclusione più coerente con tale premessa sarebbe stata quella di dichiarare la nullità del sequestro per violazione dell'art. 178 co. 1 lett. *c* c.p.p.

b. Le implicazioni del riconoscimento di un'efficacia solo indiretta all'art. 4.1 lett. c direttiva 2016/680/UE. Si ritiene preferibile, come si diceva, non riconoscere efficacia diretta all'art. l'4.1 lett. *c* direttiva. A tale impostazione aderisce un secondo filone giurisprudenziale, che, però, assume una posizione eccessivamente rigida sul punto, ritenendo che la previsione in esame non sia vincolante per il giudice interno, limitandosi ad indicare al legislatore un obiettivo da raggiungere[84].

Tuttavia, questo assunto non appare condivisibile. Indubbiamente, alle norme che presentano efficacia indiretta deve essere data attuazione nell'ordinamento interno attraverso provvedimenti normativi di recepimento, ma ciò non significa che prima della loro implementazione siano improduttive di effetti giuridici. Anzitutto, quando vengano in gioco norme non *self-executing*, incombe sul giudice nazionale l'obbligo di interpretare il diritto interno conformemente a quello europeo[85]. Naturalmente, una simile operazione ermeneutica[86] è possibile solo ove non sussista un contrasto insanabile tra le regole domestiche e quelle dell'Unione[87]. In un'ipotesi del genere, il giudice,

---

[82] In tal senso, tra i molti, AMODIO (2012), p. 3596 ss.; CAPRIOLI (2012), pp. 2444 ss.; CATALANO (2017), pp. 104 ss.; MAZZA (2015), p. 698.

[83] Sulla quale cfr., in particolare, DI PAOLO (2012), pp. 109 ss.

[84] Cass. pen., sez. VI, 4 aprile 2025, n. 17686, par. 5, nonché, in senso analogo, Cass., Sez. II, 13 novembre 2025, n. 40451, par. 2.8.2.

[85] In tal senso, tra le molte, C. giust., *von Colson*, C-14/83, 10 aprile 1984.

[86] Sulle complesse implicazioni che derivano dall'applicazione del meccanismo dell'interpretazione conforme, cfr. KOSTORIS (2025), p. 44, il quale rileva come esso integri "uno strumento molto delicato, perché è suscettibile di mettere […] in forte tensione "legalità interna" e "legalità europea"".

[87] Per la verità, non di rado il limite dell'interpretazione *contra legem* viene travalicato dalla giurisprudenza

rilevata l'antinomia, dovrebbe proporre una questione di costituzionalità delle norme interne per violazione degli artt. 11 e 117 co. 1 Cost.

In una prima sentenza, la Cassazione non sembrava ravvisare un tale conflitto, ritenendo anzi che le norme interne e le procedure in concreto seguite nell'ambito del processo *a quo* fossero compatibili con il diritto europeo[88]. Si tratta, per molti versi, di una conclusione piuttosto sbrigativa. L'art. 4.1 lett. *c* direttiva, nell'interpretazione che ne ha dato la Corte di giustizia, richiede che l'accesso ai dati contenuti in un telefono cellulare debba essere autorizzato da un giudice, mentre in Italia tale misura investigativa può essere disposta direttamente dal p.m. e, in caso d'urgenza, dalla p.g. È, dunque, evidente come sotto questo profilo non sia possibile coordinare la disciplina interna con quella europea. E non varrebbe obiettare che, come affermato dalla Cassazione, l'acquisizione dei dati sarebbe avvenuta davanti al giudice in incidente probatorio, poiché tale meccanismo, anche nell'ipotesi in cui il contraddittorio vertesse non solo sulla duplicazione del contenuto del dispositivo, ma anche sulla selezione dei dati, non equivarrebbe comunque al controllo giurisdizionale sulla richiesta di disporre il sequestro, che, come si è evidenziato, offre indubbiamente una tutela più incisiva.

Va, peraltro, evidenziato che la Suprema Corte sembra pervenire a soluzioni sostanzialmente analoghe a quella che si è poc'anzi illustrata anche ove rilevi che le regole interne non siano conformi al diritto europeo[89]. Infatti, in una seconda sentenza, la Cassazione, pur ravvisando che la mancanza di un controllo giurisdizionale *ex ante* sulla richiesta di accedere ai dati contenuti in un telefono si ponga in contrasto con l'art. 4.1 lett. *c* direttiva nell'interpretazione che ne ha dato la Corte di giustizia, ha ritenuto infondata una questione di costituzionalità della normativa interna sollevata dalla difesa in rapporto agli artt. 3 e 15 Cost. e agli artt. 7 e 8 Carta. Nel caso di specie, il ricorrente lamentava la disparità di trattamento tra la disciplina relativa all'acquisizione dei messaggi conservati in uno *smartphone*, che potrebbe essere disposta in autonomia dal p.m., e quella riguardante l'acquisizione dei tabulati telefonici, che richiederebbe, invece, la previa autorizzazione da parte del giudice (art. 132 co. 3 d.lgs. 196/2003)[90]. La Cassazione, dal canto suo, ha considerato che la previsione di modalità acquisitive differenti si giustificherebbe in ragione della diversità del loro 'oggetto': mentre l'acquisizione dei tabulati, riguardando i dati estrinseci di una comunicazione o di una

---

su sollecitazione dalla Corte di giustizia, la quale invita il giudice interno a superare il contrasto tra la norma interna e quella europea alla luce dell'intero diritto nazionale considerato nel suo complesso: v., ad es., C. Giust., *Pupino*, C-105/03, 16 giugno 2005, par. 47.

[88] Cass. pen., sez. VI, 4 aprile 2025, n. 17686, par. 5.

[89] Cass., Sez. II, 13 novembre 2025, n. 40451, par. 2.7.4.

[90] In questa prospettiva, v. già A. CHELO, *Sequestro probatorio di strumenti di comunicazione: l'imprescindibilità di una riforma*, cit., pp. 1590, secondo il quale la disciplina in materia di sequestro probatorio presentava profili di incostituzionalità anche prima della sentenza *Bezirkshauptmannschaft Landeck*, quantomeno con riferimento all'acquisizione dei dati a contenuto comunicativo. In particolare, l'Autore riteneva che costituisse una disparità di trattamento, censurabile in base all'art. 3 Cost., il fatto che l'apprensione di simili informazioni potesse essere disposta direttamente dal p.m., quando, invece, il provvedimento ablativo dei dati esterni alle comunicazioni conservati dai gestori era subordinato ad un controllo giurisdizionale *ex ante* in base all'art. 132 d.lgs. 30 giugno 2003, n. 196.

conversazione, potrebbe essere assimilata alle intercettazioni, non si potrebbe giungere alla medesima conclusione in rapporto all'estrazione dei messaggi contenuti in un telefono, i quali invece andrebbero trattati come corrispondenza e sarebbero, pertanto, acquisibili con un provvedimento di sequestro disposto dal p.m.[91].

Ragionando in questo modo, la Suprema Corte sembra, però, non tenere in dovuta considerazione il fatto che l'accesso al contenuto di uno *smartphone* rappresenta un'operazione che appare persino più intrusiva della raccolta dei dati di traffico e che quindi richiederebbe presidi analoghi, se non addirittura più forti, rispetto a quelli previsti per quest'ultimo mezzo di ricerca della prova[92].

In ogni caso, anche volendo ritenere corretta la tesi che non ritiene assimilabili le due situazioni, va evidenziato che la Cassazione, una volta rilevato il contrasto tra la disciplina interna e il diritto europeo, non avrebbe potuto limitarsi – come ha fatto – a dichiarare infondata la questione di Costituzionalità, ma avrebbe dovuto riformularla, indicando come parametri gli artt. 11 e 117 co. 1 Cost.

Infine, un ultimo rilievo: la rimessione alla Consulta non appare l'unica ipotesi percorribile. In alternativa, la Cassazione, alla luce delle diverse soluzioni ermeneutiche a cui è giunta la giurisprudenza di legittimità in rapporto alla necessità di un previo controllo giurisdizionale sul sequestro di dispositivi e dati digitali, potrebbe sollevare una questione pregiudiziale relativa all'interpretazione da attribuire all'art. 4.1 lett. *c* direttiva; il che non solo consentirebbe alla Corte di giustizia di fornire al giudice interno le coordinate necessarie ad applicare in modo corretto tale norma, verificandone al contempo la compatibilità con le regole nazionali[93], ma scongiurerebbe anche il rischio che venga avviata di una procedura di infrazione nei confronti dell'Italia.

7. I limiti di un rafforzamento del controllo giurisdizionale.

Non è agevole ipotizzare quale tra le diverse posizioni espresse dalla giurisprudenza infine prevarrà[94]. Nel complesso, si avverte un certo disagio da parte della Cassazione ad adeguarsi ad una previsione che, da un lato, implicherebbe l'ennesima forma di assoggettamento delle attività del p.m. ad un controllo giurisdizionale[95], e, dall'altro lato, correlativamente un maggiore impegno del G.I.P. nelle indagini.

---

[91] Cass., Sez. II, 13 novembre 2025, n. 40451, par. 2.7.

[92] Cfr. CAMON (2025a), p. 238. Evidenziano la sostanziale omogeneità delle due situazioni CERQUA (2026), p. 1394 e A. CHELO (2022), pp. 1588 ss.

[93] Si tratta del c.d. uso 'alternativo' del rinvio pregiudiziale: cfr., al riguardo, R.E. KOSTORIS (2025), p. 34.

[94] Nelle più recenti sentenze in materia di sequestro probatorio di dati digitali, l'attenzione della Cassazione è prevalentemente rivolta alla necessità di assicurare il rispetto del principio di proporzionalità nelle operazioni acquisitive: cfr., ad es., Cass., Sez. VI, 8 gennaio 2026, n. 543 e Cass., Sez. VI, 10 febbraio 2026, n. 15409.

[95] Si pensi, anzitutto, all'accesso ai dati di traffico conservati dai gestori, che, come si è visto, in seguito alla modifica dell'art. 132 d.lgs. 30 giugno 2003, n. 196, è subordinato all'autorizzazione da parte del giudice. Ma si assiste ad una moltiplicazione delle 'finestre giurisdizionali' anche per effetto del d.lgs. 10 ottobre 2022,

In ogni caso, occorre segnalare che è in corso di discussione in parlamento una proposta di riforma che mira a modificare le norme in materia di sequestro di dispositivi e dati digitali, introducendo un nuovo art. 254 *ter* c.p.p.[96]. La novella, oltre a recepire buona parte delle regole operative elaborate dalla giurisprudenza di legittimità[97], introduce due forme di controllo giurisdizionale sulle operazioni acquisitive. Anzitutto, il sequestro del dispositivo deve essere autorizzato con decreto motivato dal giudice su richiesta del p.m. (co. 1)[98]. Inoltre, una volta effettuato il duplicato dei dati, anche la loro acquisizione è subordinata ad un controllo giurisdizionale, ove essi integrino «comunicazioni, conversazioni o corrispondenza informatica inviate e ricevute» (co. 12)[99]. In tal modo, si vorrebbe equiparare questa operazione alle intercettazioni, come del resto emerge dal rinvio operato da questa norma agli artt. 266 co. 1 e 267 co. 1 c.p.p.: la raccolta di dati a contenuto comunicativo potrebbe, dunque, essere autorizzata dal giudice solo nell'ambito di procedimenti relativi ad illeciti che superano una certa soglia di gravità, in presenza di gravi indizi di reato e ove essa sia indispensabile ai fini della prosecuzione delle indagini.

Per le ragioni che si sono illustrate, l'esigenza di potenziare le garanzie poste a presidio del sequestro di dispositivi digitali appare ineludibile. È evidente che tale misura investigativa sia suscettibile di determinare un'invasione particolarmente significativa della sfera personale, che, per certi versi, può risultare addirittura più grave di quella prodotta dalle intercettazioni: mentre quest'ultime consentono di captare le informazioni che una persona intende condividere con altri, l'acquisizione dei dati implica potenzialmente l'accesso ad una serie di elementi che consentono di «rivelare il contenuto di intere esistenze»[100].

Anche la previsione di un controllo giurisdizionale di tipo autorizzatorio sembra – quantomeno sulla carta – rispondere a questa logica di rafforzamento delle garanzie in materia di sequestro, ma conviene fare alcune precisazioni al riguardo.

---

n. 150 (c.d. riforma Cartabia), che ha introdotto nel tessuto codicistico una serie di controlli che vertono sulla tempestività dell'iscrizione della notizia di reato, sui tempi delle indagini e sull'inerzia del p.m. quando debba adottare le determinazioni inerenti all'esercizio dell'azione penale, oltre a prevedere un'impugnazione di nuovo conio esperibile nei confronti della perquisizione che non sia seguita da un sequestro. Secondo FERRUA (2025), p. 8, il legislatore, incrementando le formalità e i controlli sulle indagini, percorre "le vie retrograde del 'garantismo inquisitorio'".

[96] Si allude al d.d.l. S.806 (c.d. d.d.l. Zanettin), che è stato approvato dal Senato e che ora è in corso di discussione alla Camera (C.1822). Su tale progetto di legge, cfr., tra i molti, CAIANIELLO (2025a); CHELO (2024); DELLA TORRE (2025); LA REGINA (2024); MALACARNE (2025b); MALACARNE (2025c), pp. 379 ss.; MURRO (2024a), pp. 253 ss.; MURRO (2024b), pp. 1619 ss.; PARODI (2024); SIGNORATO (2025).

[97] V. *supra* par. 1.

[98] In caso d'urgenza, il sequestro può essere disposto direttamente dal p.m., o, prima del suo intervento, dalla pp.g., ma deve essere comunque convalidato dal giudice (co. 4).

[99] Concetti che, per effetto del progresso tecnologico, assumono contorni sempre più evanescenti, come evidenziato da CAMON (2025a), pp. 234 ss.

[100] L'espressione è di DANIELE (2011), p. 288. In questi termini, v. anche C. Giust., *Bezirkshauptmannschaft Landeck*, cit., par. 93, secondo la quale «l'accesso a questo insieme di dati può consentire di trarre conclusioni molto precise riguardo alla vita privata della persona interessata, quali le sue abitudini di vita quotidiana, i luoghi di soggiorno permanenti o temporanei, gli spostamenti giornalieri o di altro tipo, le attività esercitate, le relazioni sociali di tale persona e gli ambienti sociali da essa frequentati».

Anzitutto, il vaglio preliminare potrebbe non assolvere autenticamente la funzione di garanzia che si auspica. Affinché esso non si traduca in un controllo meramente formale, che condurrebbe inevitabilmente ad autorizzare gran parte delle richieste presentate dal p.m.[101], occorrerebbe che il giudice disponesse del fascicolo delle indagini[102]. Tuttavia, né la Corte di giustizia né il progetto di riforma offrono indicazioni in tal senso. È, dunque, ipotizzabile che il p.m. sia libero di selezionare gli atti da allegare all'istanza che presenta al giudice. Il fatto che quest'ultimo non disponga del fascicolo integrale lo mette indubbiamente al riparo da straripamenti, ma ne sbiadisce di molto il potere di controllo[103], analogamente a quanto avviene con riferimento alla richiesta di intercettazioni, a supporto della quale l'organo d'accusa può limitarsi a produrre solo le risultanze investigative necessarie ad ottenere l'emissione del provvedimento, non essendo necessaria una piena *discovery*[104].

Si pone poi un ulteriore problema. La previsione di un'autorizzazione giurisdizionale sulla richiesta di disporre il sequestro non sostituirebbe la possibilità di impugnare il provvedimento ablativo con il riesame, ma si affiancherebbe a tale rimedio. Inoltre, ove il testo della riforma rimanesse immutato in sede di approvazione, a tali forme di controllo si aggiungerebbe, come si è accennato, quella sulla richiesta di accedere ai dati a contenuto comunicativo.

Occorre allora domandarsi se un sistema del genere sia nel complesso sostenibile. A favore di questa impostazione, si potrebbe rilevare che le due tipologie di controllo assolvono funzioni diverse: mentre un vaglio giurisdizionale *ex ante* verte esclusivamente sui presupposti del provvedimento, il riesame, dal canto suo, si estende anche alle modalità con le quali l'apprensione è avvenuta. Si potrebbe però obiettare che, con riferimento ad operazioni che determinano una grave intrusione della sfera individuale come le intercettazioni, non è previsto un controllo a posteriori di questo tipo, ma si prevede solo il divieto di utilizzare i risultati delle captazioni raccolti con modalità vietate dalla legge (art. 271 c.p.p.).

Inoltre, la moltiplicazione dei controlli sul sequestro di dispositivi e del loro contenuto potrebbe pregiudicare in maniera significativa le esigenze investigative. L'innesto di nuovi segmenti procedimentali rallenta inevitabilmente le indagini. Si tratta di una questione non trascurabile se si considera che l'intrinseca fragilità dei dati digitali imporrebbe che essi venissero raccolti in tempi brevi per evitare una loro dispersione[105]. Né la Corte di giustizia né il progetto di riforma sembrano porsi il problema, non

---

[101] Fenomeno che è segnalato anche dagli stessi magistrati assegnati all'ufficio del G.I.P.: cfr., ad es., VALORI (2018), p. 31, la quale evidenzia come sia «fisiologico che, operando di consueto *inaudita altera parte* e senza poteri integrativi, il giudice per le indagini preliminari sia indotto ad una lettura conforme a quella suggerita dal pubblico ministero».

[102] Come alcuni auspicano: v., in particolare, CASSIBBA (2024), p. 67.

[103] Si ripropone, dunque, in questo contesto, il problema – già noto all'epoca del varo del Codice del 1988 – relativo alla fisionomia del g.i.p.: un organo che dovrebbe rappresentare il garante dei diritti e delle libertà fondamentali dell'indagato, ma che, essendo privo di poteri conoscitivi, rischia di apparire in realtà come una figura sbiadita. V., in particolare, NOBILI (1991), pp. 142-143.

[104] Al riguardo, v. per tutti, CAMON (1996), pp. 92 ss.

[105] Su questo aspetto, v., in particolare, SIGNORATO (2018), pp. 132 ss.

premurandosi di indicare un termine entro il quale il giudice deve pronunciarsi sulla richiesta di sequestro del dispositivo e su quella di accesso ai dati. In un quadro di questo tipo, non si può escludere che si consolidino prassi elusive: il p.m. e la p.g. potrebbero, infatti, sistematicamente procedere all'acquisizione del *device* e del materiale informatico in autonomia, chiedendo poi la convalida al giudice e bypassando così, di fatto, il controllo giurisdizionale *ex ante*. Oltre a determinare una criticabile trasformazione di un'ipotesi eccezionale nella modalità ordinaria di procedere, un simile *modus operandi*, che marginalizza il vaglio preliminare a favore di procedure emergenziali, vanificherebbe nella sostanza l'obiettivo – sul quale la Corte di giustizia insiste in modo particolare – di scongiurare invasioni sproporzionate della sfera individuale. La mancata predisposizione di tempistiche precise per il compimento di queste attività rappresenta, dunque, un problema non di poco conto, che rischia oltretutto di riverberarsi negativamente pure sul destinatario della misura ablativa. Si pensi, ad esempio, al fatto che il progetto di riforma non prevede un termine entro il quale l'autorità giudiziaria, una volta realizzata la copia dei dati, debba procedere alla selezione dei medesimi, esponendo così «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»[106].

Non si possono, infine, trascurare i problemi che la proliferazione di controlli giurisdizionali determinerebbe sul piano organizzativo: è, infatti, ipotizzabile che il G.I.P. che autorizza il sequestro non potrebbe far parte del collegio chiamato a decidere sull'istanza di riesame, avendo già formulato una valutazione su quella misura. Non si tratta di una questione di poco conto soprattutto con riferimento ai distretti giudiziari di piccole dimensioni, o a quelli che soffrono gravi scoperture di organico[107].

8. Scenari *de iure condendo*.

Dopo aver illustrato i limiti di un sistema di controlli giurisdizionali articolato su più livelli, conviene tentare di formulare alcune proposte alternative, nella prospettiva di assicurare un equilibrato contemperamento tra la necessità di accordare un'adeguata protezione delle garanzie individuali e quella di non compromettere le esigenze investigative.

Anzitutto, si potrebbe ritenere che il vaglio giurisdizionale *ex ante* sul sequestro rappresenti un presidio irrinunciabile. In base al progetto di riforma, tale controllo è circoscritto al sequestro del dispositivo e all'acquisizione dei soli dati a contenuto comunicativo. Tuttavia, un simile approccio appare eccessivamente riduttivo. Il vaglio andrebbe, infatti, esteso anche all'accesso ai dati che non siano inquadrabili nella categoria delle 'comunicazioni'. Sarebbe, infatti, irragionevole accordare una tutela meno incisiva ad operazioni acquisitive che sono suscettibili di determinare una

[106] Così DELLA TORRE (2025).

[107] In una simile prospettiva, cfr. SIGNORATO (2025)

significativa lesione della sfera individuale[108], consentendo di raccogliere elementi che «possono consentire una ricostruzione puntuale delle abitudini di vita, dei movimenti e delle relazioni personali del soggetto interessato»[109]. Inoltre, va evidenziato che, ove non si procedesse ad un'estensione del vaglio *ex ante* all'accesso a tali informazioni, si profilerebbe un possibile contrasto della normativa interna con l'art. 4.1 lett. *c* direttiva, nell'interpretazione che ne ha dato la sentenza *Bezirkshauptmannschaft Landeck*, la quale sembra richiedere sempre un controllo giurisdizionale di tipo autorizzatorio, indipendentemente dalla natura comunicativa o meno dei dati che vengono in gioco[110].

Tuttavia, un simile sistema di controlli sarebbe sostenibile solo a patto di circoscrivere in maniera significativa la possibilità di impugnare il sequestro, che si ritiene potrebbe essere mantenuta unicamente per ottenere la restituzione del dispositivo e della copia dei dati. Negli altri casi, tale rimedio potrebbe essere sostituito da un sindacato di tipo diverso, sul modello di quello concepito dall'art. 271 c.p.p. per le intercettazioni.

In ogni caso, la previsione di un vaglio preliminare non sembra essere di per sé decisiva nella prospettiva di assicurare la protezione dei diritti individuali.

Il profilo più delicato riguarda, semmai, le garanzie partecipative. Sotto questo profilo, le dirompenti trasformazioni derivanti dalle innovazioni tecnologiche rendono per molti versi inadeguato l'attuale impianto normativo, imponendo di cercare nuovi assetti, senza però rinunciare ai valori fondanti del nostro ordinamento processuale[111], tra i quali spicca naturalmente il contraddittorio[112].

Tale obiettivo è conseguibile garantendo la piena ed effettiva partecipazione della difesa non solo alla realizzazione del duplicato del materiale informatico, ma anche, e soprattutto, alla selezione dei dati. Poiché tali operazioni avvengono nella grande maggioranza dei casi durante le indagini, si ritiene che la sede ideale per il loro svolgimento sia rappresentata dall'incidente probatorio, o comunque da un contesto processuale in cui accusa e difesa possano confrontarsi dialetticamente, anche con l'ausilio di propri consulenti, davanti ad un giudice[113]. Sotto questo profilo, la proposta di riforma appare, però, insoddisfacente, limitandosi a prevedere il contraddittorio solo con riferimento alla realizzazione del duplicato (art. 254 *ter* co. 6), senza estenderlo anche all'attività più delicata, consistente nella cernita dei dati, che resta di esclusiva pertinenza dell'autorità giudiziaria[114]. Si tratta di una scelta piuttosto singolare che

---

[108] Cfr. CAMON (2025a), pp. 238-239.

[109] In questi termini, cfr. DELLA TORRE (2025), il quale si riferisce, ad esempio, «alle immagini archiviate sul dispositivo, ai dati di geolocalizzazione, ai registri di navigazione o alle informazioni biometriche». All'interno di questa categoria di dati potrebbero pure rientrare le informazioni sanitarie o quelle relative alle preferenze sessuali, che si potrebbero ricavare anche solo dalla visualizzazione delle applicazioni installate sui dispositivi.

[110] C. Giust., *Bezirkshauptmannschaft Landeck*, cit., par. 102 ss.

[111] In tal senso, v. LUPÁRIA e ZICCARDI (2007), p. 136.

[112] "[…] regola d'oro del processo accusatorio": così FERRUA (2012), p. 2.

[113] Ove ne ricorressero le condizioni, sarebbe ammissibile anche l'espletamento di tali attività nell'ambito di un accertamento tecnico non ripetibile ai sensi dell'art. 360 c.p.p.

[114] Cfr. CAIANIELLO (2025a), nonché DELLA TORRE (2025), il quale evidenzia come un simile deficit sarebbe in

integra un'irragionevole disparità di trattamento rispetto alla materia delle intercettazioni, dove, invece, come noto, è previsto che, al termine delle operazioni captative, la difesa possa esaminare le conversazioni depositate nell'archivio e indicare quelle che ritiene rilevanti nell'ambito di un'udienza che si svolge davanti al giudice[115].

Tuttavia, va evidenziato come non sempre sia possibile celebrare un contraddittorio contestuale. Si pensi, ad esempio, all'ipotesi in cui la condivisione di determinate operazioni con l'indagato sia suscettibile di determinare un concreto pericolo per le indagini. Per non frustrare simili esigenze, il progetto di riforma[116] prevede che in situazioni del genere la duplicazione del materiale informatico possa avvenire *inaudita altera parte*, dovendosi comunque assicurare che tale attività si svolga con modalità tecniche idonee ad assicurare la conformità della copia all'originale e la sua immodificabilità (art. 254 *ter* co. 10). Si tratta indubbiamente di una garanzia importante, ma non sufficiente: dovrebbe, infatti, essere quantomeno assicurata alla difesa la possibilità di interloquire a posteriori sulle tecniche impiegate per effettuare tale operazione[117]. Non vi sarebbero poi ostacoli a garantire un contraddittorio contestuale sulla selezione dei dati[118]: tale operazione presuppone, infatti, che il materiale informatico sia stato cristallizzato con la copia, essendo così venuti meno i rischi di una sua alterazione o eliminazione.

La partecipazione della difesa costituirebbe, però, una garanzia solo apparente se ad essa non si accompagnassero due presidi fondamentali.

Anzitutto, il destinatario del sequestro deve essere informato dei motivi sui quali si fonda il provvedimento con il quale viene disposta l'acquisizione dei dati «al fine di consentirgli di difendere i suoi diritti nelle migliori condizioni possibili»[119]. La sentenza *Bezirkshauptmannschaft Landeck* richiede che tale informazione debba precedere l'accesso al materiale informatico nella prospettiva di consentire una piena tutela della riservatezza[120]. Tuttavia, è indubitabile come tale garanzia giochi un ruolo decisivo anche in funzione difensiva. Se l'indagato non conoscesse le ragioni che giustificano l'accesso ai dati, egli non potrebbe svolgere efficacemente le proprie osservazioni[121];

---

parte compensato dal nuovo art. 415 *bis* co. 2 *ter*, secondo il quale l'avviso di conclusione delle indagini dovrebbe contenere «l'avvertimento che l'indagato e il suo difensore hanno facoltà di esaminare i dati, le informazioni e i programmi oggetto di sequestro […] e il diritto alla trasposizione dei dati, delle informazioni o dei programmi medesimi su supporto idoneo».

[115] Così, ancora, CAIANIELLO (2025a), il quale auspica un'estensione di questo modello alla materia del sequestro.

[116] In base al progetto di riforma, si potrebbe derogare al contraddittorio sulla realizzazione della copia anche nell'ambito di procedimenti per i reati gravi indicati dagli artt. 406, co. 5 *bis* e 371-*bis* co. 4 *bis*, ove occorra tutelare la sicurezza nazionale, o sia necessario proteggere l'incolumità fisica e psichica di una persona.

[117] In un'analoga prospettiva, con riferimento all'acquisizione transnazionale di messaggistica, cfr. DANIELE (2025), pp. 4 e 19.

[118] Contraddittorio che, in presenza di un grave pregiudizio per le indagini, potrebbe essere eventualmente posticipato alla conclusione di tale fase, analogamente a quanto avviene per le intercettazioni (art. 415 *bis* co. 2 *bis* c.p.p.).

[119] C. Giust., *Bezirkshauptmannschaft Landeck*, cit, par. 118.

[120] *Ibidem*, parr. 120 e 122.

[121] Il destinatario della misura ablativa incontrerebbe, ad esempio, maggiori difficoltà nell'indicazione dei

garanzia quest'ultima che, come si è osservato[122], la Cassazione eleva a condizione di validità del sequestro.

Naturalmente, il diritto all'informazione non andrebbe inteso in termini assoluti, ma occorrerebbe bilanciarlo con l'esigenza di proteggere l'integrità delle indagini[123]. A tal fine, sarebbe tollerabile che l'interessato rimanesse all'oscuro delle attività sui dati in presenza di specifiche esigenze investigative. Tuttavia, una volta venute meno queste ultime, sorgerebbe l'obbligo di informare il destinatario del sequestro.

Anche sotto questo profilo, il progetto di riforma appare carente: l'indagato, infatti, non beneficia di alcuna informazione preventiva, potendo venire a conoscenza delle operazioni anche al termine delle indagini (art. 415 *bis* c.p.p.)[124].

Per altro verso, l'esercizio del diritto di difesa potrebbe essere condizionato anche dal modo in cui è stato formulato il quesito da sottoporre all'esperto chiamato ad effettuare le operazioni tecniche sui dati. A tale riguardo, conviene distinguere a seconda che tali attività vengano svolte in sede di incidente probatorio, o nell'ambito di un accertamento tecnico non ripetibile.

Nel primo caso, come noto, il giudice conferisce l'incarico al perito e formula il quesito sentite le parti e i loro consulenti (art. 226 c.p.p.). Si realizza così un confronto dialettico che contribuisce a delimitare il perimetro della questione tecnica. A tal fine, i consulenti nominati dalla difesa possono giocare un ruolo importante, presentando richieste, osservazioni e riserve (art. 230 c.p.p.), di cui «non si potrà non tenere conto in sede di controllo della perizia»[125].

Maggiori criticità pone, invece, la formulazione del quesito in sede di accertamenti tecnici irripetibili[126]. È vero che pure in questa sede è riconosciuto alla difesa, anche attraverso i propri consulenti, il potere di interloquire, ma il contraddittorio che qui si instaura risulta "imperfetto", dato che coinvolge un soggetto che forma la prova, ma che, al contempo, riveste il ruolo di parte[127]. In tal caso, il confronto dialettico potrebbe risultare meno efficace, o addirittura mancare del tutto, ove l'accertamento tecnico non ripetibile venga disposto quando ancora non è individuabile un indagato.

In situazioni del genere, non si può escludere che il quesito venga redatto in termini eccessivamente ampi. Si pensi, ad esempio, all'ipotesi in cui si domandi al consulente di svolgere le operazioni tecniche sui dati al fine di individuare elementi utili alle indagini[128]. Un quesito così generico presenterebbe un duplice ordine di problemi:

---

criteri di selezione delle informazioni e nella formulazione di critiche a quelli individuati dall'autorità giudiziaria.

[122] V. *supra* par. 5 *a*.

[123] Come riconosciuto anche da C. Giust., *Bezirkshauptmannschaft Landeck*, cit, par. 120.

[124] O, in alternativa, come evidenziato da DELLA TORRE (2025), «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.)».

[125] Così KOSTORIS (1993), p. 58.

[126] In una diversa prospettiva, v. Cass., Sez. II, 13 novembre 2025, n. 40451, par. 2.9.2, la quale invece ritiene che la procedura prevista dall'art. 360 c.p.p. tuteli pienamente le garanzie difensive.

[127] CORDERO (2012), p. 891.

[128] Prassi tollerata da una parte della giurisprudenza di merito: cfr. Trib. ord. di Venezia, Sez. dist. del

anzitutto, consentirebbe di aggirare il divieto di disporre sequestri meramente esplorativi, trasformando l'attività dell'esperto in una ricerca della notizia di reato, anziché della sua conferma; in secondo luogo, proprio tale 'mutazione genetica' delle operazioni tecniche darebbe luogo ad una riedizione di quelle prassi che si erano sviluppate nella vigenza del vecchio codice in base alle quali si attribuivano al consulente compiti che spetterebbero invece all'autorità giudiziaria[129].

A tali rilievi si potrebbe obiettare che il protocollo operativo elaborato dalla Cassazione, che, come si è osservato, è funzionale a declinare in concreto il principio di proporzionalità e che prescrive, a pena di illegittimità del vincolo, di individuare in modo preciso i dati da acquisire e le operazioni da compiere sui medesimi[130], è riferibile solo al provvedimento ablativo, non riguardando la formulazione del quesito, che avviene, invece, nell'ambito di una diversa procedura, che segue cronologicamente il sequestro al fine di darvi esecuzione.

Tale impostazione non è, però, condivisibile e appare oltretutto in contraddizione con la giurisprudenza della Suprema Corte. Va, infatti, evidenziato che la Cassazione ammette che le lacune che caratterizzano il decreto che dispone sequestro possano essere sanate quando viene conferito l'incarico all'esperto e viene definita la questione tecnica che gli viene assegnata[131]. Una simile affermazione presuppone che non sia possibile frammentare le attività probatorie, le quali, invece, vanno considerate alla stregua di un *unicum* inscindibile. Sarebbe allora irragionevole circoscrivere la portata applicativa del principio di proporzionalità al momento genetico del vincolo, dovendosi, invece, estendere anche alle operazioni tecniche svolte in esecuzione del provvedimento ablativo. In caso contrario, si consentirebbe di eludere anche le indicazioni contenute nella sentenza *Bezirkshauptmannschaft Landeck*, ammettendo di fatto la possibilità di un accesso indiscriminato ai dati da parte del consulente.

Naturalmente, l'inosservanza delle regole poste a presidio delle garanzie partecipative dovrebbe essere sanzionata con l'inutilizzabilità del materiale probatorio. Anche sotto questo profilo, la proposta di riforma appare piuttosto timida. Essa, infatti, si limita ad estendere al sequestro di dispositivi e dati digitali l'art. 271 c.p.p. in materia di intercettazioni, «in quanto compatibile». Un simile rinvio presenta una certa ambiguità. La giurisprudenza potrebbe, infatti, ritenere che esso si riferisca ai soli dati comunicativi, lasciando così scoperte le altre tipologie di dati[132].

---

riesame, ord. 14 novembre 2025.

[129] In tal senso, SIRACUSANO (1990), p. 429.

[130] V. *supra* par. 1.

[131] Cfr., tra le altre, Cass., Sez. VI, 4 febbraio 2025, n. 17479.

[132] Analogamente v. DELLA TORRE (2025).

Bibliografia

Amodio, Ennio (2012): "Il fascino ingannevole del pregiudizio effettivo (a proposito di abuso del processo)", *Cassazione penale*, pp. 3596-3598

Andolina, Elena (2021): "La sentenza della Corte di giustizia UE nel caso H.K. c. Prokuratuur: un punto di non ritorno nella lunga querelle in materia di *data retention*?", *Processo penale e giustizia*, pp. 1204-1217

Aprati, Roberta (2018): *Effettivo pregiudizio e nullità* (Padova, Cedam)

Bartoli, Laura (2018): "Sequestro di dati a fini probatori: soluzioni provvisorie a incomprensioni durature", *Archivio penale*, 1, pp. 1-24

Boldrin, Alvise (2021): "Approccio compensativo e *overall fairness* nella giurisprudenza della Corte edu, tra relativismo delle garanzie e altre derive", *La legislazione penale*, pp. 1-35.

Bolognari, Massimo (in corso di pubblicazione nel 2026): "Judicial control over the EIO in the issuing State between mutual recognition and protection of human rights"

Caianiello, Michele (2012): *Premesse per una teoria del pregiudizio effettivo nelle invalidità processuali penali* (Bologna, Bononia University Press)

Caianiello, Michele (2014): "Il principio di proporzionalità nel procedimento penale", *Rivista trimestrale di diritto penale contemporaneo*, 3-4, pp. 143-163.

Caianiello, Michele (2025): "Ancora in tema di sequestro di dispositivi, sistemi informatici o telematici o memorie digitali (disegno di legge C. 806)", *sistemapenale.it*

Caianiello, Michele (2025): "Il principio di proporzionalità nel processo penale", *Rivista italiana di diritto e procedura penale*, pp. 1003-1016

Caianiello, Michele, Manes, Vittorio (2020): *Introduzione al diritto penale europeo. Fonti, metodi, istituti, casi*, (Torino, Giappichelli)

Camon, Alberto (2017): "Cavalli di Troia in Cassazione", *Archivio della nuova procedura penale*, pp. 91-100

Camon, Alberto (2025): "I confini mobili delle intercettazioni", *Diritto penale e processo*, pp. 232-239

Camon, Alberto (2025): "Le prove", in Camon, Alberto, Cesari, Claudia, Daniele, Marcello, Di Bitonto, Maria Lucia, Negri Daniele, *Fondamenti di procedura penale*, V ed. (Padova, Wolters Kluwer – Cedam), pp. 325-438

Caprioli, Francesco (2012): "Abuso del diritto di difesa e nullità inoffensive", *Cassazione penale*, pp. 2444-2463

Caprioli, Francesco (2017): "Il captatore informatico come strumento di ricerca della prova in Italia", *Revista brasileira de direito processual penale*, pp. 483-510

Cascone, Giulia (2022): "La Corte di Giustizia dell'Unione Europea definisce le condizioni per la legittimità delle normative nazionali in materia di acquisizione dei tabulati. Le ripercussioni sull'ordinamento italiano della sentenza del 2 marzo 2021 (C-746/18) nel caso H.K.", *Cassazione penale*, pp. 419-440

Cassibba, Fabio (2024): ""Trasfigurazione" delle indagini preliminari, principio di proporzionalità e controllo giurisdizionale effettivo", in Gaito, Alfredo, Voena, Giovanni (a cura di), *Ricordando Giovanni Conso* (Pisa, Pisa University Press), pp. 61-72.

Catalano, Elena Maria (2017): "Le invalidità alla deriva", *Rivista italiana di diritto e procedura penale*, pp. 104-126

Ceresa Gastaldo, Massimo, Lonati, Simone (2021): *Profili di procedura penale europea*, (Milano, Giuffrè)

Cerqua, Federico (2026): "Sequestro probatorio informatico: il cortocircuito tra norme interne e diritto UE", *Cassazione penale*, pp. 1381-1395

Chelo, Andrea (2022): "Sequestro probatorio di strumenti di comunicazione: l'imprescindibilità di una riforma", *Diritto penale e processo*, pp. 1583-1592

Chelo, Andrea (2024): "Tanto tuonò che piovve: il nuovo sequestro di dispositivi informatici", *penaledp.it*

Conso, Giovanni (1955): *Il concetto e le specie di invalidità. Introduzione alla teoria dei vizi degli atti processuali penale* (Milano, Giuffrè)

Cordero, Franco (1961): "Nullità, sanatorie e vizi innocui", *Rivista italiana di diritto e procedura penale*, pp. 680-732

Cordero, Franco (2012): *Procedura penale*, IX ed. (Milano, Giuffrè)

Curtotti, Donatella (2024): "Brevi note in tema di proporzionalità del decreto di sequestro probatorio", *Giurisprudenza italiana*, pp. 2700-2703

Daniele, Marcello (2011): "La prova digitale nel processo penale", *Rivista di diritto processuale*, pp. 283-298.

Daniele, Marcello (2021): "L'immediatezza in crisi. Mutazioni pericolose ed anticorpi accusatori", *Sistema penale*, 2, pp. 53-71

Daniele, Marcello (2023): "Ordine europeo di indagine penale e comunicazioni criptate: il caso Sky ECC/Encrochat in attesa delle Sezioni Unite", *sistemapenale.it*

Daniele, Marcello (2025): "Oei e messaggi digitali già acquisiti all'estero. Riflessioni a partire dal caso Sky ECC", *Sistema penale*, pp. 1-33

Della Torre, Jacopo (2025): "Spunti di riflessione sulla proposta di legge in materia di sequestro di dispositivi e di dati", *sistemapenale.it*

Di Paolo, Gabriella (2012): *La sanatoria delle nullità nel processo penale* (Padova, Cedam)

Dinacci, Filippo (2025): "Sequestro di dispositivi informatici: imposizioni tecnologiche e scelte interpretative. Alla ricerca di un recupero della legalità probatoria", *Archivio penale web*

Donini, Massimo (2011): *Europeismo giudiziario e scienza penale. Dalla dogmatica classica alla giurisprudenza-fonte* (Milano, Giuffrè)

Ferrua, Paolo (1997): "Declino del contraddittorio e garantismo reattivo: la difficile ricerca di nuovi equilibri processuali", in Ferrua, Paolo, *Studi sul processo penale, III, Declino del contraddittorio e garantismo reattivo* (Torino, Giappichelli)

Ferrua, Paolo (2012): *Il «giusto processo»* (Bologna, Zanichelli)

Ferrua, Paolo (2020): "La lenta agonia del processo accusatorio a trent'anni dall'entrata in vigore: trionfante nella Carta costituzionale, moribondo nel reale", *Processo penale e giustizia*, pp. 7-15

Ferrua, Paolo (2025): "La magistratura tra processo accusatorio e separazione delle carriere", *Discrimen*, pp. 1-11

Filippi, Leonardo (2024): "La CGUE mette i paletti all'accesso ai dati del cellulare", *Quotidiano giuridico*

Galantini, Novella (1999): voce "Vizi degli atti processuali", *Digesto delle discipline penalistiche*, vol. XV, pp. 340-367

Giordano, Luigi (2026): "Accesso della polizia giudiziaria ai dispositivi elettronici", *Ius penale*

Kostoris, Roberto E. (1993): *I consulenti tecnici nel processo penale* (Milano, Giuffrè)

Kostoris, Roberto E. (2011): "Ricerca e formazione della prova elettronica: qualche considerazione introduttiva", in Picotti, Lorenzo, Ruggieri, Francesca (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica* (Torino, Giappichelli), pp. 179-182

Kostoris, Roberto E. (2020): "Per una "grammatica" minima del giudizio di equità processuale", *Rivista italiana di diritto e procedura penale*, pp. 1675-1698

Kostoris, Roberto E. (2020): "Una grave mistificazione inquisitoria: la pretesa fede privilegiata del responso del consulente tecnico dell'accusa", *sistemapenale.it*

Kostoris, Roberto E. (2025): "Diritto europeo e giustizia penale", in Kostoris, Roberto E. (a cura di), *Manuale di procedura penale europea*, VI ed. (Milano, Giuffrè), pp. 1-85

Lasagni, Giulia (2018): "Tackling Phone Searches in Italy and the United States: Proposals for a Technological Rethinking of Procedural Rights and Freedoms", *New Journal of European Criminal Law*, pp. 386-401

Lupária, Luca, Ziccardi, Giovanni (2007): *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali* (Milano, Giuffrè)

Malacarne, Alessandro (2021): "La decretazione d'urgenza del Governo in materia di tabulati telefonici: breve commento a prima lettura del d.l. 30 settembre 2021, n. 132", *Sistema Penale*.

Malacarne, Alessandro (2025): "La Cassazione sul sequestro dello smartphone: la disciplina italiana non è conforme al diritto dell'UE (… ma il materiale raccolto è comunque utilizzabile)", *Sistema Penale.*

Malacarne, Alessandro (2025): "Sequestro probatorio (informatico): proporzionalità, segreto professionale e garanzie dell'attività difensiva", *Diritto di internet*, pp. 131-140

Malacarne, Alessandro (2025): ""Tentativo di accesso" ai dati contenuti nello smartphone: le (ondivaghe) indicazioni provenienti dalla Corte di giustizia", *Rivista italiana di diritto e procedura penale*, pp. 373-381

Malacarne, Alessandro, Tessitore, Gaia (2022): "La ricostruzione della normativa in tema di *data retention* e l'ennesima scossa della Corte di giustizia: ancora inadeguata la disciplina interna?", *Archivio penale*, 3, pp. 1-45

Marcolini, Stefano (2022): "La disciplina processuale italiana sulla data retention", in Flor, Roberto, Marcolini, Stefano (a cura di), *Dalla* data retention *alle indagini ad alto contenuto tecnologico* (Torino, Giappichelli), pp. 35-73

Mazza, Oliviero (2015): "Il pregiudizio effettivo tra legalità processuale e discrezionalità del giudice", *La giustizia penale*, III, pp. 697-704

Mazza, Oliviero (2019): "Il sarto costituzionale e la veste stracciata del codice di procedura penale", *Archivio penale*, 2, pp. 1-7

Murro, Ottavia (2024): *Lo smartphone come fonte di prova. Dal sequestro del dispositivo all'analisi dei dati* (Padova, Cedam)

Murro, Ottavia (2024): "Prospettive in tema di sequestro dello smartphone: le novità approvate dal Senato", *Diritto penale e processo*, pp. 1619-1630

Nicolini, Mario (2026): "La Cassazione torna sul tema del sequestro finalizzato all'acquisizione di prove digitali consolidando l'evoluzione dello statuto del PM come organo di giustizia", *Sistema Penale.*

Nobili, Massimo (1991): "Diritto alla prova e diritto di difesa nelle indagini preliminari", in Aa.Vv., *Il nuovo processo penale dalla codificazione all'attuazione. Dalla codificazione all'attuazione. Atti del Convegno presso l'Università di Bari. Ostuni, 8-10 settembre 1989* (Milano, Giuffrè), pp. 129-148

Orlandi, Renzo (2018): "Usi investigativi dei cosiddetti captatori informatici. criticità e inadeguatezza di una recente riforma", *Rivista italiana di diritto e procedura penale*, pp. 538-556

Palma, Isidoro (2026): "Il sequestro di materiale informatico d'iniziativa del pubblico ministero o della polizia giudiziaria è incompatibile con le garanzie comunitarie?", *Cassazione penale*, pp. 2111-2120

Panzavolta, Michele, Maes, Elise (2022): "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", *The International Journal of Evidence & Proof*, vol. 26(3), pp. 199-222

Parlato, Lucia (2018): "Problemi insoluti: le perquisizioni *on-line*", in Giostra, Glauco, Orlandi, Renzo (a cura di), *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche* (Torino, Giappichelli), pp. 289-323

Parodi, Cesare (2024): "Signori, si cambia: la nuova disciplina sul sequestro di p.c. e *device*", *ilpenalista.it*

Paulesu, Pier Paolo (2014): "Riflessioni sul ruolo del criterio del pregiudizio effettivo nell'ambito delle nullità processuali in una prospettiva costituzionalmente orientata e alla luce della giurisprudenza europea", *Rivista di diritto processuale*, pp. 882-896

Paulesu, Pier Paolo (2023): "Invalidità processuali penali e scenari in trasformazione: tensioni antiformalistiche, efficienza, garanzie", in Catalano, Elena Maria, Ferrua, Paolo (a cura di), *Corderiana. Sulle orme di un maestro del rito penale* (Torino, Giappichelli), pp. 293-309

Pittiruti, Marco (2021): "Dalla Corte di cassazione un vademecum sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali *omnibus*", *Sistema Penale.*

Rafaraci, Tommaso (1998): voce "Nullità (dir. proc. pen.)", *Enciclopedia del diritto*, Agg. II, pp. 597-627

Schiavone, Susanna (2026): "L'incompetenza funzionale del p.m. travolge il sequestro probatorio", *Cassazione penale*, pp. 161-171

Signorato, Silvia (2018): *Le indagini digitali: profili strutturali di una metamorfosi investigativa* (Torino, Giappichelli)

Signorato, Silvia (2024): "Dalla immediatezza alla mediatezza: un moto oscillatorio che investe anche la copia forense", in S. Signorato (a cura di), *L'immediatezza nel processo penale* (Milano, Giuffrè), pp. 157-166

Signorato, Silvia (2025): "Il sequestro di dispositivi e informazioni digitali", *Sistema Penale.*

Siracusano, Delfino (1990): "Le prove", in Siracusano, Delfino, Dalia, Andrea, Galati, Antonio, Tranchina, Giovanni, Zappalà, Enzo, *Manuale di diritto processuale penale*, vol. 1 (Milano, Giuffrè), p. 371-456

Torre, Marco (2026): "Sequestro probatorio dello *smartphone*: il principio di proporzionalità assurge a canone di legittimità dell'ingerenza", *Diritto penale e processo*, pp. 505-516

Valori, Chiara (2018): "Pubblico ministero e giurisdizione nelle indagini e nell'esercizio dell'azione penale: il punto di vista del giudice per le indagini preliminari", *Questione giustizia*, 1, pp. 30-33.