# QUESTIONI APERTE

## Indagini digitali

**La decisione**
**Tentativo di accesso – Cellulare - *E-Evidence* - Indagini digitali - Diritto di difesa - Controllo preventivo – Giudice - Autorità amministrativa indipendente – Comunicazioni – Perquisizione – Sequestro - Riservatezza** (Artt. 7; 8; 11; 41; 47; 52 CDFUE; artt. 1, 3, 5; 15 direttiva (UE) 2002/58; artt. 2; 3; 4; 6; 10; 13; 54 direttiva (UE) 2016/680; artt. 14; 15, 24; 111 Cost.; d.lgs. 18 maggio 2018, n. 51).
*L'articolo 4, paragrafo 1, lettera c), della direttiva 2016/680/UE (sulla tutela delle persone fisiche riguardo al trattamento dei dati personali in ambito penale), letto alla luce degli articoli 7, 8 e 52, paragrafo 1, CDFUE, non osta ad una normativa nazionale che riconosca alle autorità competenti la possibilità di accedere ai dati contenuti in un telefono cellulare, per scopi di prevenzione, indagine, accertamento e perseguimento di reati, anche non necessariamente gravi, purché tale normativa definisca in modo sufficientemente preciso la natura o le categorie dei reati interessati, garantisca il rispetto del principio di proporzionalità e sottoponga l'esercizio di tale facoltà – salvi i casi di urgenza debitamente motivati – ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente;*
*Gli artt. 13 e 54 della direttiva 2016/680/UE ostano ad una normativa nazionale che autorizzi le autorità competenti a tentare l'accesso ai dati contenuti in un telefono cellulare senza informare la persona interessata dei motivi posti a fondamento dell'autorizzazione ad accedere a tali dati, rilasciata da un giudice o da un organo amministrativo indipendente, a partire dal momento in cui la comunicazione di tali informazioni non sia più tale da compromettere le indagini.*
CORTE DI GIUSTIZIA, GRANDE CAMERA, 4 ottobre 2024, C.G. c. Bezirkshauptmanschaft Landeck (C-548/21).

### Nuove garanzie europee per l'acquisizione della prova digitale

Con la sentenza in epigrafe, la Corte di Giustizia UE qualifica come "trattamento" dei dati personali, ai sensi della direttiva 2016/680, il tentativo di accesso a un telefono cellulare operato a scopo investigativo. Il contributo si propone di rintracciare eventuali antinomie tra diritto interno e diritto unionale, esaminando criticamente i potenziali effetti che, a partire dalla pronuncia, si riverberano in ambito domestico, anche alla luce di un'inedita ordinanza, emessa – da ultimo – dal Tribunale di Milano.

*New european guarantees for the acquisition of digital evidence*

*With this judgment, the EUCJ qualifies as 'processing' of personal data, within the meaning of Directive 2016/680, the attempted access to a mobile phone operated for investigative purposes. The contribution aims to trace possible antinomies between Italian and EU law, critically assessing the potential effects of the ruling in the domestic sphere, also in the light of an unpublished decision issued by the Court of Milan.*



1. *La controversia nella causa principale*. Il caso in esame origina dal sequestro e dal successivo tentativo di accesso a un telefono cellulare effettuati dalla polizia doganale austriaca, su personale iniziativa dei medesimi agenti[1], nel contesto di un'indagine concernente la detenzione e il traffico di sostanze stupefacenti[2].

Tali operazioni erano state espletate a seguito del diniego opposto dal soggetto interessato a fronte della richiesta di fornire i codici che avrebbero consentito lo sblocco del dispositivo mobile. Quest'ultimo, quindi, adiva il giudice del Landesverwaltungsgericht, Tribunale amministrativo regionale del Tirolo, contestando la legittimità della misura. Solo nell'ambito di tale procedimento, a seguito della testimonianza resa da un agente di polizia coinvolto, l'interessato apprendeva dei diversi tentativi di estrazione dei dati contenuti nel proprio cellulare, non essendo stati tali tentativi documentati nell'informativa redatta dalla polizia giudiziaria.

In ragione di ciò, il Tribunale proponeva rinvio pregiudiziale alla Corte di Giustizia *ex* art. 267 TFUE, con riferimento a talune questioni che ci si appresta a illustrare.

2. *Le questioni pregiudiziali.* In primo luogo, ritenendo applicabile al caso di specie la direttiva 2002/58, concernente la tutela del diritto alla vita privata e

[1] Cfr. punto n. 23 della sentenza.

[2] Nella fattispecie, l'oggetto di contestazione era l'art. 27, n. 1 della Suchtmittelgesetz (Legge sugli stupefacenti) del 5 settembre 1997 (BGBl. I, 112/1997), in relazione al rinvenimento, da parte dei funzionari dell'Ufficio delle Dogane di Innsbruck, di 85 grammi di cannabis contenuti all'interno di un pacco indirizzato al soggetto che, a seguito della perquisizione effettuata presso la sua abitazione, subiva il sequestro del telefono cellulare.

alla riservatezza delle comunicazioni elettroniche[3], il giudice del rinvio rimetteva alla Corte di Giustizia l'interpretazione del suo art. 15 § 1, che regola la possibilità per gli Stati membri di prevedere adeguate limitazioni a taluni diritti sanciti dalla normativa europea, anche in presenza di esigenze di prevenzione, ricerca, accertamento e perseguimento dei reati[4].

In particolare, si domandava se la richiamata disposizione, alla luce del combinato disposto con gli artt. 7 e 8 della CDFUE, relativi, rispettivamente, alla tutela della vita privata e familiare nonché alla protezione dei dati personali, dovesse essere letta nel senso che l'attività investigativa espletata dalle autorità pubbliche sui dati conservati nei telefoni cellulari comporta un'ingerenza, nei già richiamati diritti fondamentali, di gravità tale da limitare l'accesso in materia di prevenzione, ricerca, accertamento e perseguimento dei reati, alla lotta della criminalità grave.

In proposito, si evidenziava, da un lato, come il compendio digitale contenuto nel cellulare fosse potenzialmente in grado di veicolare informazioni molto dettagliate e approfondite di ogni aspetto della vita privata del soggetto interessato; dall'altro, invece, si precisava che l'art. 27 n. 1 della legge austriaca sugli stupefacenti, oggetto di contestazione nel procedimento principale, costituendo una fattispecie incriminatrice "minore", fosse possibilmente inidonea a giustificare l'apprensione totalizzante dei dati personali dell'accusato.

In secondo luogo, il giudice rimettente interpellava la Corte in ordine alla corretta interpretazione del disposto del suddetto art. 15 § 1, letto alla luce degli artt. 7, 8, 11, 52 § 1 della Carta di Nizza, con riferimento al combinato disposto degli artt. 18 e 99 § 1 del codice di rito penale austriaco (StPO). Nel dettaglio, si chiedeva se la norma di diritto europeo osti a una normativa na-

[3] Il riferimento è alla direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche.

[4] Art. 15 § 1, direttiva 2002/58: «Gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all´articolo 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell´articolo 13, paragrafo 1, della direttiva 95/46/CE, una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell´uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l'altro adottare misure legislative, le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo. Tutte le misure di cui al presente paragrafo sono conformi ai principi generali del diritto comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea.»

zionale in forza della quale «le autorità preposte alla sicurezza si procurano autonomamente, nel corso di un'indagine penale, l'accesso completo e incontrollato a tutti i dati digitali contenuti in un telefono cellulare, senza l'autorizzazione di un tribunale o di un organo amministrativo indipendente».
In terzo e ultimo luogo, il giudice europeo veniva interrogato in merito alla compatibilità del combinato disposto dei citati artt. 18 e 99 § 1 StPO con il principio di parità delle armi e il diritto a un ricorso giurisdizionale effettivo, sanciti dall'art. 47 CDFUE, anche alla luce degli artt. 41 e 52 della medesima Carta. Il quesito mirava a chiarire se le invocate disposizioni di diritto europeo ostano a una normativa nazionale che consente «di analizzare digitalmente un telefono cellulare senza che l'interessato ne sia informato preventivamente o, almeno, successivamente all'esecuzione della misura».
Si segnala che la Corte di Giustizia ha proceduto a riformulare le illustrate questioni alla luce della direttiva 2016/680, in quanto ritenuta pertinente nel caso di specie.

3. *Sull'applicabilità della direttiva 2016/680.* Preliminarmente, la Corte lussemburghese ha valutato l'opportunità di applicare alla controversia nella causa principale, alternativamente, la direttiva 2002/58, come ipotizzato dal Tribunale austriaco, ovvero la direttiva 2016/680[5], relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati[6].
In proposito, il giudice europeo ha chiarito che, sulla base della prevalente interpretazione invalsa nella giurisprudenza della Corte di Giustizia[7], la direttiva 2002/58 viene in rilievo qualora gli Stati membri attuino misure derogatorie del principio di riservatezza delle comunicazioni, imponendo obblighi di trattamento ai fornitori di servizi di tali comunicazioni; diversamente, nelle

[5] Direttiva (UE) 2016/680 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.
[6] Cfr. i punti nn. 69 ss. della sentenza.
[7] Cfr. il punto n. 57 della sentenza che rinvia a: Corte Giust. UE, 6 ottobre 2020, Privacy International, C-623/17, EU:C:2020:790, punto n. 48; 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791, punto n. 103.

ipotesi in cui non sia prescritto l'intervento di tali operatori, trova applicazione la direttiva 2016/680.
Ne è derivato che, difettando nella fattispecie il coinvolgimento di un fornitore di servizi di comunicazione elettronica, quest'ultima sia stata ricondotta all'ambito applicativo della direttiva 2016/680, con la conseguente riformulazione dei primi due quesiti pregiudiziali ad opera della stessa Corte[8].
Quanto a questi ultimi, tuttavia, il governo austriaco ha presentato eccezione di incompetenza, dolendosi dell'estraneità della direttiva 2016/680 al quadro normativo tracciato dal giudice del rinvio; inoltre, ha lamentato l'irritualità di una nuova formulazione delle questioni pregiudiziali, sostenendo che le disposizioni di diritto austriaco che avevano sollecitato l'intervento pretorio (artt. 5 e 15 della direttiva 2002/58) non trovassero corrispondenza nella direttiva 2016/680.
Nel respingere tale eccezione, il giudice del Kirchberg ha evocato il principio di leale cooperazione tra le Corti, il quale esige che la pronuncia emanata all'esito della procedura *ex* art. 267 TFUE permetta all'organo di giurisdizione nazionale di dirimere la controversia che gli è stata sottoposta. In questa prospettiva, la Corte di Giustizia è ammessa a riformulare le questioni devolutele anche alla luce di normative unionali che, sebbene non espressamente contemplate dal giudice rimettente, siano comunque ritenute pertinenti nel caso concreto.

3.1. *Le argomentazioni della Corte.* Al fine di valutare se il tentativo della polizia di accedere ai dati del telefono cellulare rientri nel perimetro applicativo della direttiva 2016/680, la Corte ha preso le mosse dal disposto dell'art. 2 § 2 che ne circoscrive l'applicazione al «trattamento dei dati personali da parte delle autorità competenti», in particolare, per «finalità di prevenzione, indagine, accertamento e perseguimento di reati».
Successivamente, ha valorizzato la lettera art. 3, punto 2 della direttiva che fornisce la definizione di «trattamento». A ben vedere, infatti, in ragione della sua ampia formulazione, la norma consente di estendere la latitudine applicativa della direttiva a «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o

[8] Cfr. punti nn. 56 ss. della sentenza.

insiemi di dati personali, come [...] l'estrazione, la consultazione» o la «diffusione o qualsiasi altra forma di messa a disposizione».
Inoltre, la circostanza che la direttiva fosse caratterizzata da una portata ampia è stata dedotta dal catalogo meramente esemplificativo delle «operazioni», o «insieme di operazioni», idonee a integrare un trattamento dei dati personali ai sensi della suddetta disposizione. Sintomatico, in questo senso, è l'uso del vocabolo «come» che prelude – per l'appunto – a una elencazione non tassativa delle possibili operazioni aventi ad oggetto i dati personali, rappresentando sotto questo profilo una valvola di apertura nel sistema di tutela congegnato dal legislatore europeo.
In ragione di questi elementi, la Corte ha ritenuto che il sequestro e la successiva manipolazione di un telefono cellulare da parte delle autorità di polizia, per finalità di estrazione e consultazione dei dati personali *ivi* contenuti, configurano operazioni idonee a integrare un «trattamento» ai sensi dell'art. 3, punto 2 della direttiva 2016/680. Per giunta, considerato il quadro sistematico in cui la richiamata disposizione si inscrive, anche il solo tentativo, benché infruttuoso, di accedere a tali dati è sussumibile nella nozione di «trattamento». Sul punto, è stato evidenziato che, a garanzia dell'effettività del principio che sancisce la "limitazione delle finalità di raccolta dei dati personali", di cui all'art. 4 § 1, lett. *b)*[9] della direttiva in discorso, è necessario che queste ultime siano predefinite sin dalla fase del tentativo di accesso dal momento che, nell'eventualità in cui l'intrusione si fosse rivelata proficua, i dati sarebbero entrati nell'immediata disponibilità dell'autorità investigativa.
Del resto, a parere della Corte, una lettura di segno diverso avrebbe condotto allo svilimento dell'obiettivo, connaturato alla direttiva 2016/680, di assicurare un elevato livello di protezione dei dati personali delle persone fisiche[10]. Così, ove il "tentato accesso" fosse rimasto fuori dal perimetro del concetto di "trattamento", la direttiva avrebbe finito per costituire solo un'arma spuntata a fronte del significativo rischio per la platea di soggetti interessati di perdere irrimediabilmente il controllo sui propri dati.
A conforto di tale lettura depongono, infine, i principi di certezza del diritto e di prevedibilità, i quali impongono di delimitare a priori l'ambito applicativo

[9] In forza di tale principio, i dati personali possono essere raccolti solo per finalità determinate, esplicite e legittime e trattati in modo non incompatibile con tali finalità.
[10] Cfr. il punto n. 74 della sentenza che richiama a sua volta i considerando nn. 4,7,15 della direttiva.

della normativa, evitando così di far dipendere una simile opera definitoria dalla buona riuscita del tentativo di accesso al dispositivo mobile.

4. *Sulla prima e seconda questione*. Nell'esaminare congiuntamente la prima e la seconda questione oggetto di rinvio, entrambe afferenti all'interpretazione dell'art. 15 § 1 della direttiva 2002/58, la Corte ha ritenuto di poterle rimodulare alla luce della corrispondente disposizione di cui all'art. 4 § 1, lett. *c)* della direttiva 2016/680[11]: mentre la prima presidia il rispetto della proporzionalità delle misure volte a limitare l'esercizio dei diritti previsti dalla normativa europea, la seconda tutela la proporzionalità nella raccolta dei dati che, in ossequio al principio di "minimizzazione", devono essere adeguati, pertinenti e non eccessivi rispetto alle finalità del trattamento.
Sicché, a seguito della riformulazione, si è domandato se l'art. 4 § 1, lett. *c)* della direttiva 2016/680, letto alla luce degli artt. 7, 8 e 52 § 1 della Carta di Nizza, osti a una normativa nazionale che consenta alle autorità competenti di accedere ai dati contenuti in un telefono cellulare, per la prevenzione, ricerca, accertamento e perseguimento dei reati, senza assoggettare tale prerogativa ad un preventivo controllo da parte di un giudice o di un organo amministrativo indipendente.
Per fornire una risposta sul punto, la Corte ha dapprima sviluppato un'argomentazione funzionale, fondata sull'analisi degli obiettivi perseguiti dalla direttiva 2016/680.
Quest'ultima è volta a costruire un quadro giuridico solido e coerente in materia di protezione dei dati personali che rinsaldi le guarentigie previste dal diritto primario dell'Unione[12]. In questo contesto, peraltro, la direttiva mira ad assicurare – da un lato – un elevato livello di protezione del compendio di dati personali nel doveroso rispetto dei diritti fondamentali e a contribuire – dall'altro – alla realizzazione di uno spazio di libertà, sicurezza e giustizia[13].
Tuttavia, la Corte ha osservato che, non costituendo il diritto alla protezione dei dati personali e il diritto al rispetto della vita privata e familiare prerogative assolute dell'individuo, debbano conseguentemente soggiacere alle eventuali limitazioni derivanti dal bilanciamento con altri diritti fondamentali.

[11] Cfr. i punti nn. 78-80 della sentenza.
[12] Si allude all'art. 8 § 1, C.D.F.U.E. e all'art. 16 § 1, T.F.U.E. che sanciscono il diritto universale alla protezione dei dati di carattere personale.
[13] Cfr. i considerando nn. 2 e 4 della direttiva 2016/680.

L'applicabilità di tali restrizioni è condizionata al rispetto delle regole previste dall'art. 52 § 1 CDFUE il quale impone che queste ultime siano prescritte per legge, preservino il contenuto essenziale del diritto e rispettino il principio di proporzionalità, potendo essere previste solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'UE o all'esigenza di proteggere i diritti e le libertà altrui.
Si è proceduto, quindi, a svolgere una più dettagliata disamina dei presupposti sanciti dalla Carta di Nizza al fine di valutare se, nel limitare l'esercizio dei diritti in questione, le previsioni normative venute in rilievo nel caso di specie fossero conformi al diritto UE.
In primo luogo, è necessario che le eventuali limitazioni siano previste da una norma chiara e precisa che ne disciplini la portata e l'applicazione, predefinendo, per natura o per categoria, i reati che abilitano l'autorità ad ingerirsi nella sfera privata dell'interessato[14].
In secondo luogo, la Corte ha chiarito che l'azione investigativa diretta alla repressione di un reato, come quella occorsa nel caso di specie, rientra nella nozione di «finalità di interesse generale», richiamata dall'art. 52 CDFUE. Nondimeno – ha soggiunto la Corte – tale requisito non appare soddisfatto quando «l'obiettivo di interesse generale perseguito sia ragionevolmente conseguibile in modo altrettanto efficace con altri mezzi, meno pregiudizievoli per i diritti fondamentali degli interessati»[15]. Pertanto, occorre che il trattamento dei dati personali rappresenti l'*extrema ratio* nel ventaglio delle soluzioni volte a conseguire la medesima finalità di interesse generale.
In terzo luogo, la Corte ha vagliato la sussistenza del requisito della proporzionalità, ponderando «tutti gli elementi pertinenti del caso di specie»[16]. Tra questi, assumono particolare rilevanza la gravità della limitazione, a sua volta desunta dalla natura e dalla sensibilità dei dati personali oggetto del trattamento, dall'importanza dell'obiettivo di interesse generale cui il trattamento è diretto nonché dal legame che avvince il proprietario del telefono cellulare e il reato perseguito.

[14] Cfr. i punti nn. 98 e 99 della sentenza.
[15] Cfr. il punto n. 87 della sentenza.
[16] Corte Giust. UE, 30 gennaio2024, Direktor na Glavna direktsia «Natsionalna politsia» pri MVR – Sofia, C-118/22, EU:C:2024:97; 22 novembre 2022, Luxembourg Business Registers, C-37/20 e C-601/20, EU:C:2022:912.

Con riguardo al primo parametro, il tentativo di accesso ai dati contenuti nel dispositivo dell'interessato si è rivelato sintomatico di un'interferenza particolarmente grave nei diritti fondamentali garantiti dagli artt. 7 e 8 CDFUE, in considerazione delle modalità con cui è stata svolta l'operazione investigativa e della speciale sensibilità dei dati potenzialmente rinvenibili nel dispositivo mobile. A tale riguardo, è stato evidenziato che la normativa austriaca non contempla la previa formalizzazione di un'autorizzazione, quale presupposto del tentativo di accesso, con il conseguente rischio che siano perpetrati atti arbitrari da parte dell'autorità investigativa. In difetto di un atto autorizzatorio, del resto, i presupposti e i limiti del trattamento non trovano preventiva definizione, dipendendo unicamente dalle scelte operate dagli agenti. Il che, osserva la Corte, espone l'interessato a una lesione potenzialmente più seria dei propri diritti alla protezione dei dati personali e al rispetto della vita privata e familiare, in quanto non è possibile escludere a priori che il cellulare contenga dati sensibili dell'interessato. Né, alle già menzionate condizioni, sembra possibile applicare le più robuste garanzie di liceità di trattamento enunciate dall'art. 10 della direttiva 2016/680 in relazione a questa particolare categoria di dati personali[17].

Con riferimento al secondo requisito, «l'importanza dell'obiettivo perseguito» è stata parametrata alla gravità del reato oggetto di indagine. Pertanto, almeno sotto questo profilo, la proporzionalità dell'ingerenza nell'esercizio del diritto, è assicurata laddove sia stata intrapresa un'azione di contrasto per gravi reati.

Sennonché, come ha evidenziato il giudice europeo, se ci si limitasse a legittimare il tentativo di accesso ai dati personali solo in relazione a tali ipotesi, rimarrebbero pregiudicate le esigenze punitive legate alla commissione di altri reati, con implicazioni sicuramente più modeste ma comunque rilevanti, ove sol si considerino gli obiettivi e la complessiva *ratio* della direttiva 2016/680.

Quanto al terzo presupposto, la sussistenza di un «legame tra il proprietario del telefono cellulare e il reato oggetto dell'indagine» è stata vagliata alla luce

[17] Cfr. l'art. 10, direttiva 2016/680: «Il trattamento di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, e il trattamento di dati genetici, di dati biometrici intesi a identificare in modo univoco una persona fisica o di dati relativi alla salute o di dati relativi alla vita sessuale della persona fisica o all'orientamento sessuale è autorizzato *solo se strettamente necessario*, soggetto a *garanzie adeguate per i diritti e le libertà dell'interessato* e soltanto: *a)* se autorizzato dal diritto dell'Unione o dello Stato membro; *b)* per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica; o *c)* se il suddetto trattamento riguarda dati resi manifestamente pubblici dall'interessato.»

della nozione di "interessato", di cui all'art. 6 lett. *a)* della direttiva in questione. Tra questi soggetti, titolari dei dati personali oggetto di trattamento, sono ricomprese «le persone per le quali vi sono fondati motivi di ritenere che abbiano commesso o stiano per commettere un reato», sicché, in base alla formulazione della norma, è necessario che l'esistenza di ragionevoli sospetti nei confronti dell'indagato «sia suffragata da elementi oggettivi e sufficienti».
A garanzia dei principi che assicurano la legittimità del trattamento, ha sostenuto la Corte, la sussistenza dei vari indici denotativi della sua proporzionalità deve essere valutata alla stregua di un controllo preventivo effettuato da un giudice o da un organo amministrativo indipendente. A tal fine, è essenziale che l'autorità controllante disponga di pieni poteri e di tutte le garanzie necessarie ad assicurare il bilanciamento dei legittimi interessi in gioco: da un lato, le esigenze connesse ad un corretto sviluppo dell'indagine e, dall'altro, il rispetto dei diritti fondamentali contemplati dalla normativa europea.
Inoltre, con specifico riferimento alla controversia oggetto della causa principale, è stata evidenziata l'opportunità che il controllo intervenga prima di qualsiasi tentativo di accesso ai dati personali, salvo che ricorrano casi di urgenza debitamente comprovati a fronte dei quali, ad ogni modo, il controllo deve avvenire in tempi brevi.
L'operazione di accesso, pertanto, presuppone la formulazione da parte delle autorità investigative di una domanda motivata diretta all'organo indipendente che, a seguito dell'espletamento di un controllo a monte, è ammesso a rifiutare o a limitare tale accesso ove ritenga che, alla luce della direttiva 2016/680, l'ingerenza nei diritti fondamentali dell'interessato risulti sproporzionata o comunque non in linea con i requisiti stabiliti dalla normativa europea.
Infine, l'organo controllante assume il dovere di verificare la sussistenza delle condizioni rafforzate di liceità previste dall'art. 10 della direttiva 2016/680 qualora l'ambito del trattamento si estenda, anche solo in via potenziale, a particolari categorie di dati, come i dati sensibili. In tali casi, infatti, il rilascio dell'autorizzazione è subordinato all'effettuazione di un vaglio particolarmente rigoroso in ordine alla stretta necessità di procedere al trattamento.
Alla luce di questi elementi, la pronuncia ha isolato tre condizioni in presenza delle quali una normativa nazionale che conceda alle autorità competenti la possibilità di accedere ai dati contenuti in un telefono cellulare, a fini di prevenzione, ricerca, accertamento e perseguimento di reati possa ritenersi conforme al diritto UE: *1)* che la natura o le categorie dei reati in relazione ai

quali sia possibile effettuare tali operazioni siano predefinite in modo sufficientemente preciso; *2)* che sia assicurato il rispetto del principio di proporzionalità nel trattamento dei dati; *3)* che, salvo in casi di urgenza debitamente comprovati, il tentativo di accesso sia subordinato al controllo preventivo di un giudice o di un organo amministrativo indipendente.

5. *Sulla terza questione.* La terza questione oggetto di rinvio pregiudiziale è stata riformulata alla luce degli artt. 13 e 54 della direttiva 2016/680, ritenuti corrispondenti alle disposizioni originariamente invocate dal giudice austriaco e concernenti, rispettivamente, le informazioni che gli Stati membri devono rendere disponibili all'interessato e il diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento. Pertanto, a seguito della rimodulazione effettuata dalla Corte di Giustizia, si è domandato se le previsioni della direttiva in questione, lette alla luce dell'art. 47[18] e 52 § 1 della Carta di Nizza, ostino ad una normativa nazionale che consente alle autorità investigative di accedere ai dati contenuti in un telefono cellulare senza informare l'interessato.
Al fine di fornire riscontro sul punto, la Corte si è essenzialmente attenuta al disposto delle richiamate disposizioni di diritto derivato.
Da un lato, infatti, ha preso in considerazione il dettato dell'art. 13 della direttiva 2016/680 che, nel definire il novero delle informazioni che il titolare del trattamento deve rendere all'interessato, stabilisce l'obbligo di fornirne di ulteriori, in particolare, nel caso in cui i dati personali siano raccolti all'insaputa di quest'ultimo (§ 2, lett. *d*). Nondimeno, per bilanciare detto obbligo, la norma autorizza il legislatore nazionale a escludere o limitare la comunicazione di informazioni all'interessato laddove tali omissioni siano funzionali a salvaguardare il corso dell'indagine (§ 3, lett. *a), b).*
D'altro canto, ha attenzionato la previsione di cui all'art. 54 della direttiva 2016/680 che, mutuando il principio sancito dall' art. 47 CDFUE, assicura il diritto dell'interessato a un ricorso giurisdizionale effettivo in presenza di una violazione delle prerogative riconosciutegli dalla direttiva, perpetrata a seguito del trattamento dei dati di cui è titolare.
Pertanto, fermo restando la necessaria previsione di un obbligo informativo in capo alle competenti autorità nazionali, è necessario che l'oggetto

[18] L'art. 47 CDFUE. regola il diritto a un ricorso effettivo e a un giudice imparziale.

dell'informativa sia costituito dai motivi sui quali si fonda l'autorizzazione allo svolgimento del trattamento dei dati personali, di modo da consentire all'interessato di esercitare il proprio diritto a un ricorso effettivo. Sono fatte salve le limitazioni che rispettino i presupposti sanciti dall'art. 52 § 1 CDFUE: che siano previste per legge, rispettino il contenuto minimo del diritto e rispondano al principio di proporzionalità nonché a finalità di interesse generale. Il rilascio dell'informativa è altresì subordinato alla circostanza che le operazioni investigative non ne siano conseguentemente compromesse.
Alla luce di queste argomentazioni, la Corte ha interpretato gli artt. 13 e 54 della direttiva 2016/680,
nel senso che «ostano a una normativa nazionale che autorizza le autorità competenti a tentare di accedere a dati contenuti in un telefono cellulare senza informare l'interessato, nell'ambito dei procedimenti nazionali applicabili, dei motivi sui quali si fonda l'autorizzazione ad accedere a tali dati, rilasciata da un giudice o da un organo amministrativo indipendente, a partire dal momento in cui la comunicazione di tale informazione non rischia più di compromettere i compiti spettanti a dette autorità in forza di tale direttiva».

*6. Profili di frizione con il diritto interno.* La sentenza in commento assume significativa importanza in considerazione degli effetti che potrebbe sortire in ambito domestico.
In primo luogo, spicca l'innovativa interpretazione della nozione di "dati personali" di cui all'art. 3 punto 1 della direttiva 2016/680. A parere del giudice europeo, infatti, quest'ultima si estende fino a ricomprendere ogni informazione custodita nella memoria di un telefono cellulare purché sia in grado di rivelare aspetti della vita privata e familiare del suo proprietario, quali, ad esempio, le sue abitudini di vita, i luoghi di soggiorno, gli spostamenti giornalieri, le attività esercitate e le sue relazioni sociali.
Si tratta, a ben vedere, di una nozione teleologicamente orientata, caratterizzata da geometrie suscettibili di variazioni in ragione dell'attitudine informativa del dato. Astrattamente, infatti, tutte le informazioni contenute in uno *smartphone* possono rappresentare "dati personali" nell'accezione delineata dalla Corte, compresi – *a fortiori* – dati personali "sensibili", come tali suscettibili di disvelare le prerogative più intime della persona.
Nondimeno, il fattore differenziale, che permette di distinguere un dato personale dalla generalità di informazioni custodite in un cellulare, si sostanzia

nella capacità del dato di squarciare il velo dell'intimità del suo titolare. Tanto più eloquente è l'informazione, maggiore è la protezione che la normativa europea le accorda.

In questa prospettiva, per così dire funzionalizzata, integrano il concetto di "dato personale" le informazioni rinvenibili in un dispositivo mobile che riguardano il traffico telefonico, l'ubicazione, le fotografie, la cronologia di navigazione su Internet, finanche le comunicazioni contenute nei messaggi che vi sono conservati[19]. Di fatti, come ha sostenuto la Corte, «l'accesso a questo insieme di dati può consentire di trarre conclusioni molto precise riguardo alla vita privata della persona interessata»[20].

Alla luce di questa esegesi e considerata l'assenza di coinvolgimento da parte di fornitori di servizi di comunicazioni, prende corpo l'intuizione del giudice europeo: tali informazioni ricadono nel raggio applicativo della direttiva 2016/680, con le garanzie che ne conseguono.

Tra le prime implicazioni osservabili sul piano sistematico, viene in rilievo la qualificazione giuridica della messaggistica custodita nella memoria di uno *smartphone*[21], ricollegata – da ultimo – alla nozione di "corrispondenza"[22] *ex* art. 15 Cost., per effetto della nota sentenza della Corte costituzionale n. 170/2023[23]. A far base sull'interpretazione elaborata in quest'ultima decisione, nel pieno rispetto dei *dicta* europei[24], la tutela delle comunicazioni elettroni-

[19] Cfr. punto n. 92 della sentenza.

[20] Punto n. 93 della sentenza.

[21] Si precisa che la natura del "contenitore" dei dati informatici non è rilevante, potendo indifferentemente trattarsi di telefoni cellulari, di computer o di altri dispositivi elettronici. In tal senso, Corte cost., n. 270/2023, punto n. 5.5 del Considerato in diritto.

[22] Propende per un concetto unitario di "corrispondenza": TORRE, *Considerazioni su perquisizione, sequestro e intercettazioni digitali*, in *Dir. pen. proc.*, 6/2024, 811 ss.

[23] Corte cost., 27 luglio 2023, n. 170, con commento di CHELO, *Davvero legittimo il sequestro di messaggi e-*mail *e* WhatsApp *già letti?*, in *Giur. cost.*, 2023, 1746; CURTOTTI, *La sentenza costituzionale n. 170 del 2023 e le comunicazioni "apparenti": quando un eccesso di garanzie non sempre è un moltiplicatore di garanzie*, in *Dir. inform.*, 2023, 4/5, 708 ss. Si v., inoltre, FILIPPI, *Il cellulare "contenitore" di corrispondenza anche se già letta dal destinatario*, in *www.penaledp.it*, 6 settembre 2023, 475; FONTANI, *La svolta della Consulta: la "corrispondenza telematica" è pur sempre corrispondenza*, in *Dir. pen. proc.*, 10/2023, 1311 ss.; LUPÀRIA DONATI-CERQUA, *La versione della Consulta sulla corrispondenza elettronica: un* "bouleversement" *in materia di prova digitale?*, *Dir. inform.*, 4-5/2023, 718-729; ORLANDI, "*Corrispondenza" dei parlamentari e limiti all'accertamento penale: appunti critici sulla sentenza nr. 170 del 2023 della Corte costituzionale*, in *Dir. inform.*, n. 4-5/2023, 730-737.

[24] Cfr. Corte cost., n. 170/2023, punto n. 4.4 del Considerato in diritto, in cui si richiamano: CEDU, sentenza "Copland", § 44; con riguardo alla messaggistica istantanea, CEDU, sentenza "Barbulescu, §

che, intese nella loro dimensione "statica", non si esaurisce con la ricezione del messaggio da parte del destinatario, perdurando altresì fin tanto che esso conservi carattere di attualità e interesse per gli interlocutori[25].

Detto assunto sembrerebbe destinato a conoscere un auspicabile sviluppo sulla scia del *decisum* emanato dalla Corte di Giustizia: sul presupposto che le comunicazioni elettroniche sono potenzialmente idonee a configurare "dati personali" ai sensi della direttiva 2016/680, infatti, a queste ultime dovrebbe essere accordata la protezione derivante dalla normativa europea in virtù della loro attitudine a conculcare il diritto alla riservatezza dell'interessato, indipendentemente dalla circostanza che preservino carattere di attualità e interesse per gli interlocutori.

In secondo luogo, la portata innovatrice della pronuncia si apprezza con riferimento all'ampliamento della corrente nozione di "trattamento" dei dati personali, permeata nel diritto interno per il tramite del d.lgs. 18 maggio 2018, n. 51[26] di attuazione della direttiva 2016/680[27].

Per effetto dell'interpretazione resa dal giudice europeo, infatti, quest'ultima assume contorni ben più ampi, inglobando – a definizione immutata – anche il tentativo di accedere ai dati personali contenuti in un telefono cellulare. Più precisamente, ad avviso della Corte di Giustizia, l'immissione in un sistema elettronico, benché in forma tentata, è attratta nel fuoco della direttiva 2016/680 in quanto potenziale viatico per la consultazione o l'apprensione del compendio informativo *ivi* conservato.

Da questo insperato approdo discende che il tentativo intrusivo sorretto da finalità investigative debba soggiacere ai presupposti di legittimità del trattamento dei dati personali, con macroscopiche ripercussioni sulla disciplina

---

74; con riguardo a dati memorizzati in *floppy disk*, Corte EDU, Sez. V, 22 maggio 2008, "Iliya Stefanov c. Bulgaria", § 42; sul sequestro dei dati di uno *smartphone*, Corte EDU, sentenza Saber, § 48.

[25] Così, Corte cost., n. 170/2023, punto n. 4.4 del Considerato in diritto: «Si deve dunque concludere che, analogamente all'art. 15 Cost., quanto alla corrispondenza della generalità dei cittadini, anche, e a maggior ragione, l'art. 68, terzo comma Cost. tuteli la corrispondenza dei membri del Parlamento – ivi compresa quella elettronica – anche dopo la ricezione da parte del destinatario, almeno fino a quando, per il decorso del tempo, essa non abbia perso ogni carattere di attualità, in rapporto all'interesse alla sua riservatezza, trasformandosi in un mero documento "storico".»

[26] Cfr. l'art. 2, co. 1, lett. *b)* d.lgs. 18 maggio 2018, n. 51 di attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

[27] Cfr. l'art. 3 punto 2 della direttiva 2016/680.

processuale che regola, a livello domestico, l'attività di ricerca della prova digitale[28].

Contrariamente a quanto stabilito dalla Corte del Lussemburgo, infatti, la disciplina interna si astiene dal selezionare preventivamente la natura o le categorie di reati a fronte dei quali è consentito procedere alla ricerca dell'*e-evidence*; né subordina il tentativo di accesso ad un controllo effettuato *ex ante* da parte di un giudice o di un organo amministrativo indipendente. Tanto è vero che l'accesso alla memoria del dispositivo, che sia operato sulla scorta dell'art. 247 ovvero dell'art. 352, co. 1-*bis* c.p.p., è disposto o convalidato con decreto motivato dal pubblico ministero, il quale rientra, secondo un consolidato indirizzo esegetico, nella nozione di "autorità giudiziaria"[29].

Nel vigore di questa interpretazione, del resto, non è consentito pervenire a soluzioni differenti, neppure qualificando le comunicazioni elettroniche come "corrispondenza" *ex* art. 15 Cost., giacché, in applicazione della richiamata disposizione costituzionale, ogni limitazione al diritto alla segretezza delle comunicazioni è ammessa per atto motivato dell'"autorità giudiziaria", complessivamente intesa[30], e non già di un giudice o di un'autorità indipendente[31].

---

[28] Ampiamente, sul tema, si v. CURTOTTI, *Attività di acquisizione della* digital evidence*: ispezioni, perquisizioni e accertamenti tecnici*, in *Cyber forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici*, Torino, 2021, 439 ss.; FELICIONI, *Le ispezioni e perquisizioni di dati e sistemi*, in *Cybercrime*, Torino, 2023, 1587 ss.; MANCUSO, *L'acquisizione di contenuti e-mail*, in *Le indagini atipiche*, SCALFATI *(a cura di)*, Torino, 2019, 502 ss.; MARANDOLA, *Sequestro informatico. Ambito: finalità probatorie e adempimenti successivi*, in *Dir. Pen. Proc.*, 2/2021, 211 s.; MONTI, *La nuova disciplina del sequestro informatico*, in *Sistema penale e criminalità informatica,* a cura di Luparia Donati, Milano, 2009,198-199; PITTIRUTI, Digital evidence *e procedimento penale*, Torino, 2017, 33 ss., in cui l'A. evidenzia come nel disciplinare l'attività di ricerca dell'*e-evidence*, il legislatore, piuttosto che enucleare le modalità operative sul dato informatico, abbia inteso assicurarne la conservazione e l'immodificabilità nonché la conformità all'originale; TONINI, *Documento informatico e giusto processo*, in *Dir. pen. proc.*, 4/2009, 401 ss.

[29] In tal senso, CAMON, *Le intercettazioni nel processo penale*, Milano, 1996, 109; ILLUMINATI, *La disciplina processuale delle intercettazioni*, Milano, 1983, 61, nt. 16; RUGGIERI, *Divieti probatori e inutilizzabilità nella disciplina delle intercettazioni telefoniche*, Milano, 2001, 10, nt. 11. In proposito, CAPRIOLI, *Intercettazioni e tutela della* privacy *nella cornice costituzionale*, in *Cass. pen.*, 2021, 1141, il quale osserva che «l'art. 15 Cost. non contiene un'autentica riserva di giurisdizione».

[30] Com'è noto, al sequestro di corrispondenza *ex* art. 254 può procedere anche «il pubblico ministero indagante»: cosi, CORDERO, *Procedura penale*, IX ed., Milano, 2012, 839.

[31] Dalla riconduzione delle comunicazioni elettroniche al concetto di "corrispondenza" *ex* art. 15 Cost. discende che la polizia giudiziaria non può prenderne cognizione mediante sequestro *ex* art. 354, co. 2, c.p.p., potendo procedere al sequestro del solo "contenitore" nelle forme e nei modi dell'art. 254, co. 2 c.p.p. al fine di consegnarlo all'autorità giudiziaria: ALBANESE, *La "nuova" corrispondenza nel processo penale, tra recenti sviluppi giurisprudenziali e scenari* de lege ferenda, in *Dir. pen. proc.*, 11/2024, 1517

Tale impostazione, tuttavia, sembra collidere con la posizione, ribadita anche di recente dal giudice lussemburghese[32], a tenore della quale in capo al pubblico ministero non sarebbero ravvisabili i requisiti di indipendenza e imparzialità che l'autorità incaricata di esercitare il controllo preventivo deve soddisfare. A tal fine, evidenzia la Corte, sarebbe necessario che quest'ultima, «da un lato, non [fosse] coinvolta nella conduzione dell'indagine penale di cui trattasi e, dall'altro, [avesse] una posizione di neutralità nei confronti delle parti del procedimento penale»[33].

D'altro canto, le delineate carenze nella disciplina interna sembrerebbero incidere anche sul piano del controllo di proporzionalità[34] che, secondo i dettami della Corte di Giustizia, deve essere effettuato sul trattamento dei dati da un'autorità indipendente. Al contrario, nel nostro ordinamento questo è affidato all'organo dell'accusa che, nell'autorizzare l'espletamento della misura volta alla ricerca della prova, emana un decreto (non più precisamente) motivato al fine di circoscrivere i limiti relativi a detta attività di indagine (cfr. artt. 244 ss. c.p.p.).

Non può trascurarsi, tuttavia, che nella vaghezza del dato normativo, la giurisprudenza di legittimità abbia continuamente valorizzato l'onere motivazione del pubblico ministero, ricercando – nel nome della proporzionalità – una composizione armonica tra la doverosa tutela dei diritti individuali e le esigenze legate all'efficacia delle indagini[35]. Con riferimento ai c.d. decreti *omni-*

---

ss. A tal riguardo appaiono significative, Cass., Sez. un., 29 febbraio 2024, n. 23755 e 23756 i cui principi sono stati ribaditi da: Cass., Sez. II, 28 giugno 2024, n. 25549, § 1.1.5 e §1.1.6.; Id., Sez. VI, 21 maggio 2024, n. 31180, con commento di MARANDOLA, *Chat SMS whatsapp: serve il provvedimento dell'autorità giudiziaria*, *Giur. it.*, 1/2025, 178 ss.

[32] Tra i più recenti arresti, Corte Giust. UE, Grande Camera, 2 marzo 2021, *H. K.* c./*Prokuratuur*, C-746/18, in materia di conservazione di dati relativi al traffico telefonico/informatico; con nota di BATTARINO, *CGUE e dati relativi al traffico telefonico e telematico. Uno schema di lettura*, in *www.questionegiustizia.it*. Cfr., inoltre, FILIPPI, *La Grande Camera della Corte di giustizia U.E. boccia la disciplina italiana sui tabulati*, in *www.penaledp.it*, 8 Marzo 2021.

[33] In particolare, si rinvia ai punti nn. 54-57, sentenza Corte Giust. UE, Grande Camera, *H. K.* c./*Prokuratuur*, C-746/18.

[34] Sulla proporzionalità in relazione agli atti d'indagine CAMON, *La prova genetica tra prassi investigative e regole processuali*, in *Proc. pen. giust.*, 167; NICOLICCHIA, *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, in *www.archiviodpc.dirittopenaleuomo.org*, 8 gennaio 2018; SIGNORATO, *Indagini e prove digitali,* in *Riv. di Dir. Proc.*, 4/2024, 1152; UBERTIS, *Prova penale e proporzionalità*, in *www.sistemapenale.it., 23 gennaio 2025.*

[35] Tra le altre, cfr. Cass., Sez. I, 23 gennaio 2025; Cass., Sez. II, 4 ottobre 2023, n. 46130, Santandrea; Cass., Sez. VI, 24 ottobre 2019, n. 43556, con nota di NULLO, *Sequestro probatorio di materiale do-*

*bus*, in particolare, ha precisato che il rispetto del principio di proporzionalità deve essere parametrato al livello di approfondimento e dettaglio della motivazione che, per quanto concisa, dia conto specificatamente della finalità perseguita per l'accertamento dei fatti[36]. Del pari, è stato ritenuto dirimente che, ai fini dell'assolvimento dell'onere di motivazione, il provvedimento del pubblico ministero rechi un contenuto minimo volto a delimitare il profilo «quantitativo, qualitativo e temporale» dell'atto investigativo[37].

Peraltro, qualora l'attività di ricerca della prova consista in particolare nel tentativo di accesso a sistema elettronico, tali parametri andrebbero integrati alla luce degli elementi valutativi presi in considerazione dal giudice europeo: la gravità dell'atto intrusivo, a sua volta desunta dalla natura e dalla sensibilità dei dati personali oggetto di trattamento, dall'obiettivo di interesse generale cui il trattamento è diretto nonché dal legame che avvince il proprietario del dispositivo al reato perseguito.

In disparte gli sforzi interpretativi profusi dai supremi giudici, resta comunque evidente il *vulnus* che la disciplina processuale presenta dinanzi alle pretese garanzie di imparzialità del soggetto preposto al controllo di proporzionalità. Permangono dubbi, in altri termini, in merito alla circostanza che l'organo deputato al ruolo di parte processuale nel perseguire la funzione d'accusa, possa tradurre in un effettivo bilanciamento le contrapposte esigenze connes-

---

*cumentativo e principi di adeguatezza e proporzionalità*, in *Proc. pen. giust.*, 3/2020, 660 ss.; Cass., VI Sez., 17 luglio 2019, n. 31593, con nota di PITTIRUTI, *Adeguatezza e proporzionalità nel sequestro di un sistema informatico,* in *Dir. di Internet, 24 luglio 2019;* Sez. VI, 12 settembre 2018, n. 56733. Cfr. anche, TORRE, *Indagini informatiche e principio di proporzionalità*, in *Proc. pen. e giust.*, 6/2019, ss.

[36] Cass., Sez. Un., 27 luglio 2018, n. 36072 – Pres. Carcano; Rel. Andreazza, punto n. 6 del Considerato in diritto, con nota di GRAMUGLIA, *Le Sezioni Unite tornano sui confini dell'onere di motivazione del decreto di sequestro probatorio del* corpus delicti, in *www.archiviodpc.dirittopenaleuomo.org*, 27 settembre 2018; CORTESI, *Sequestro del corpo del reato e onere motivazionale: dopo un tormentato dibattito interpretativo raggiunto "forse" un punto fermo*, in *Proc. pen. giust.*, 1/2019, 150 ss.

[37] A pena di illegittimità del decreto, occorre che il provvedimento sia specificamente motivato in ordine al nesso di pertinenza tra bene appreso e ipotesi investigativa; in relazione alla tipologia di operazioni tecniche da svolgere sul dato e con riguardo alla durata temporale del vincolo. Così: Cass., Sez. VI, 2 dicembre 2020, n. 34265, con nota di PITTIRUTI, *Dalla Corte di cassazione un* vademecum *sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali* omnibus, in *www.sistemapenale.it,* 14 gennaio 2021, § 4; Sez. VI, 15 febbraio 2024, n. 17312, con commento di CURTOTTI, *Brevi note in tema di proporzionalità del decreto di sequestro probatorio*, in *Giur. it.*, 12/2024, 2698 ss.

se al corretto sviluppo dell'indagine, da un lato, e al rispetto dei diritti fondamentali, dall'altro[38].

Infine, la sentenza in commento sollecita un'ulteriore riflessione con riferimento al passaggio in cui si asserisce che chi patisce un tentativo di accesso al proprio cellulare a scopo investigativo debba essere preventivamente informato, per mezzo di un'informativa rilasciata da un giudice o da un'autorità amministrativa indipendente, dei motivi sui quali si fonda l'autorizzazione a compiere l'atto[39].

Fin qui, al netto di alcune oscillazioni, la barra rimane sostanzialmente ferma: la perquisizione e il sequestro di un telefono cellulare, finalizzati – rispettivamente – alla consultazione o all'estrazione dei dati in esso contenuti, sono effettuate, seppur a sorpresa, in modo palese e garantito[40]. Considerando che lo scopo di queste attività non è – come per le intercettazioni *ex* art. 266 *bis* c.p.p. – il monitoraggio occulto, bensì la ricerca palese della prova[41], la disciplina processuale prevede espressamente che l'interessato sia reso edotto del relativo compimento (artt. 250; 253, co. 4; 352, co. 4; 355, co. 1 c.p.p.). Tuttavia, a dispetto di quanto sancito dalla sentenza del giudice europeo, la disciplina codicistica impone che gli sia consegnata/notificata copia del decreto di sequestro o di convalida emesso dal pubblico ministero e non già da un giudice o da un organo amministrativo indipendente.

---

[38] In merito alla "cultura della giurisdizione", come "cultura del decidere" propria del giudice, anche in ordine alla compressione della sfera di riservatezza del privato, MAZZA, intervento nell'ambito del panel *P.M. parte imparziale e la cultura della giurisdizione*, *Inaugurazione dell'anno giudiziario dei penalisti italiani 2025*, Milano - 7 febbraio 2025, min. 2.23.

[39] Salvo che il diritto dell'interessato sia limitato in conformità ai dettami dell'art. 52 CDFUE. o comprometta il buon esito dell'indagine.

[40] Viene in rilievo il c.d. "criterio funzionale", valorizzato dalla Consulta (Corte cost., n. 170/2023), al fine di distinguere tra intercettazioni e sequestro. Tale criterio si fonda sulle modalità di esecuzione dell'atto investigativo: qualora l'attività captativa sia effettuata da remoto e in modo occulto si dà luogo a un'intercettazione; viceversa, qualora l'attività investigativa, seppur a sorpresa, sia eseguita in modo palese e garantito, si configura un sequestro. In tema, PITTIRUTI, *Profili processuali della prova informatica*, in *Incontri ravvicinati" con la prova penale. Un anno di seminari a Roma Tre*, a cura di Marafioti, Paolozzi, Torino, 2014, 59; DE FLAMMINEIS, *Le intercettazioni telematiche*, in *Dir. pen. proc.*, 2013, 992; ORLANDI, *Questioni attuali in tema di processo penale e informatica*, in *Riv. dir. proc.*, 2009, 135.

[41] Nel differenziare intercettazioni e sequestri, si suole agganciare il "criterio funzionale" a quello dello "scopo dell'atto": l'attività di captazione è svolta in maniera occulta poiché il fine dell'attività investigativa è il monitoraggio senza soluzione di continuità; l'attività di estrazione dei dati è operato in maniera scoperta e garantita poiché lo scopo non è il monitoraggio occulto, ma la ricerca palese. Così, TORRE, *Considerazioni su perquisizione, sequestro e intercettazioni digitali*. cit., 811 ss.

Come rammenta la Corte di Giustizia, la conoscenza del provvedimento è funzionale ad assicurare all'interessato il diritto a un ricorso effettivo, garantito nel nostro ordinamento dall'accesso al riesame (art. 257 c.p.p.[42]), anche a seguito della restituzione del *device* sequestrato, da cui sia stata estratta la copia forense dei dati informatici *ivi* custoditi[43]. Sotto questo profilo, la disciplina interna appare pienamente conforme al diritto unionale: resta solo da immaginare se, in sede di proposizione del gravame, verrà effettivamente ritenuto concreto ed attuale l'interesse dedotto dal ricorrente il quale abbia subito un mero tentativo di accesso al proprio cellulare, poi rivelatosi infruttuoso.

7. *Una prima pronuncia, ancora conservativa, della giurisprudenza interna.* Talune statuizioni espresse nella sentenza in esame sono state invocate per la prima volta a livello domestico, nell'ambito di un procedimento di riesame *ex* art. 324 c.p.p., in relazione al decreto con cui il p.m. disponeva il sequestro dei telefoni cellulari in uso all'indagato con la finalità di esaminarne la memoria[44].

In difesa di quest'ultimo, si adduceva, per quanto qui d'interesse, che l'apprensione dei dati contenuti nel cellulare dovesse avvenire con le garanzie imposte dalla direttiva 680/2016 per come interpretata dalla CGUE. Pertanto, si evidenziava che la legittimità dell'accesso ai dispositivi fosse condizionata alla sussistenza di una previsione nazionale che, da un lato, circoscriva le gravi ipotesi di reato a fronte delle quali procedere e che, dall'altra, imponga al giudice, e non già al p.m., l'emanazione del provvedimento di autorizzazione all'espletamento dell'atto investigativo. In ragione di ciò, la difesa perorava la disapplicazione della normativa interna (d.lgs. n. 51/2018) in quanto essa non

[42] Per un commento all'art. 257 c.p.p., SELVAGGI, in *Commento al nuovo codice di procedura penale*, CHIAVARIO *(a cura di),* vol. II, Torino, 1990, 750 ss.: «la previsione del riesame del provvedimento disposto a fini probatori [...] intende soddisfare all'esigenza di predisporre un sistema di controllo su qualsiasi provvedimento che si presenti astrattamente idoneo a incidere su diritti garantiti a livello costituzionale (diritto di proprietà e libertà di iniziativa economica)»; TRANCHINA, (voce) *Sequestro penale*, in *Enc. giur.*, vol. XXVIII, 6.

[43] Cass., Sez. un., 20 luglio 2017, Andreucci, ric., con commento di BARTOLI, *Sequestro di dati a fini probatori: soluzioni provvisorie a incomprensioni durature*, in *Arch. pen. web,* 1/2018. Descrive bene il passaggio da un quadro giuridico improntato all'apprensione di *res* tangibili a un nuovo assetto caratterizzato dalla immaterialità degli elementi di prova e delle prove SIGNORATO*, Indagini e prove digitali.* cit., 1152.

[44] Trib. Milano, Sez. XII, ord., 18 dicembre 2024.

subordina l'apprensione a tali requisiti, sollecitando, in alternativa, il giudice del riesame a sollevare questione pregiudiziale ai sensi dell'art. 267 TFUE.
Nel rigettare i suddetti motivi di doglianza, il giudice del riesame, pur ravvisando talune antinomie con il diritto unionale, non ha ritenuto di dover disapplicare la normativa nazionale, demandando l'incomodo all'intervento del legislatore: dato il tenore del *decisum* europeo, spetterebbe a quest'ultimo definire i presupposti legittimanti il trattamento dei dati, in adesione al principio di leale cooperazione (art. 4 § 3, TUE).
L'approdo, in realtà, sembra riposare su una lettura abnorme del richiamato principio che, com'è noto, nel governare i rapporti tra l'UE e le istituzioni statuali[45], proietta in capo al giudice l'obbligo[46] di interpretare la normativa nazionale in conformità al diritto UE. Del resto, in un sistema multilivello che aspira ad offrire garanzie pur senza attuare una sincronica armonizzazione fra ordinamenti, è fondamentale che «l'interprete cerchi di dare alle singole disposizioni il senso che meglio le faccia coesistere con tutte le altre»[47]. Nondimeno, l'ordinanza che ci occupa riflette una postura diametralmente opposta: anziché scegliere la via maestra dell'interpretazione conforme con le altre leggi, sembra che si preferisca accettare passivamente situazioni di contrasto, smarcandosi – in ultima analisi – anche dalla più opportuna soluzione del rinvio pregiudiziale.
Infine, il giudice *de quo* ha ritenuto che il disposto della CGUE non fosse suscettibile di inficiare la legittimità dell'attività investigativa espletata, considerato che l'effettuazione del sequestro ha preceduto il momento in cui è stata emanata detta decisione. Sicché, in applicazione del principio *tempus regit actum*, il Tribunale ha valorizzato il momento dello svolgimento dell'attività funzionale all'assunzione della prova, con la conseguenza di escludere ogni effetto della sentenza del giudice europeo sulla legittimità di tali operazioni.
In quest'ultimo snodo argomentativo, tuttavia, il giudice del riesame sembra trascurare due importanti aspetti. Da un lato, che al momento del compimento delle attività d'indagine, fosse già entrata in vigore la direttiva 680/2016;

[45] CARTABIA, *L'attività della Corte costituzionale nel 2019*, in *www.cortecostituzionale.it*, 28 aprile 2020, 6.
[46] Cfr. BIN, *L'interpretazione conforme. Due o tre cose che so di lei*, dall'intervento al convegno "*L'interpretazione conforme al diritto UE. Profili e limiti di un vincolo problematico",* Rovigo, 15- 16 maggio 2014: l'A. osserva come l'interpretazione conforme, quale canone dell'interpretazione giuridica, configuri, piuttosto che un "obbligo", una pratica consigliata al fine di evitare il contrasto fra norme.
[47] *Idem.*

dall'altro, che l'interpretazione elaborata dalla Corte di Giustizia in ordine alle fonti di diritto UE, avendo natura di interpretazione autentica, possiede efficacia retroattiva. In definitiva, la circostanza che la sentenza sia stata emanata in un momento successivo rispetto all'espletamento delle attività di indagini, non appare idonea a giustificare l'inapplicabilità del *decisum* al caso di specie.

8. *Note conclusive.* La sentenza in commento conduce a un significativo avanzamento sul piano della tutela dell'indagato che subisca l'accesso del proprio *smartphone* per finalità investigative.
La riconduzione dell'atto – finanche del tentativo di accesso – sotto l'egida della direttiva 680/2016, infatti, implica che gli siano riconosciute le garanzie che la normativa europea accorda al soggetto "interessato" a fronte del "trattamento" dei suoi dati personali. Tra queste riveste particolare interesse la necessità che l'atto investigativo sia preceduto da un provvedimento autorizzatorio emanato da un giudice o da un'autorità amministrativa indipendente, alla luce delle potenziali ricadute sul diritto interno.
D'altro canto, è necessario tenere in considerazione un dato di contesto. Le posizioni espresse dal giudice europeo non si presentano isolate. Al contrario, possono iscriversi in un più ampio dibattito in ordine al bilanciamento dei rapporti tra difesa e pubblica accusa, di cui è espressione – in ambito domestico – l'intento di inserire nel codice di rito penale il nuovo art. 254-*ter*, che introduce una disciplina *ad hoc* sul sequestro di *smartphone* e altri dispositivi[48]. Sembra, infatti, che sulla scia tracciata dalla Corte costituzionale, con la sentenza n. 170/2023, anche l'azione legislativa si stia muovendo verso l'apertura di nuove finestre di giurisdizione nel perimetro delle indagini digitali[49]. In questa prospettiva, pertanto, la sentenza in commento può essere letta come un inedito enunciato di quel dibattito che depone a favore del rafforzamento delle garanzie individuali dell'indagato.

**SUSANNA SCHIAVONE**

[48] Cfr. MAZZA, *Col ddl smartphone passi avanti, ma non basta: garanzie ancora a rischio*, in *www.ildubbio.news,* 11 aprile 2024.
[49] Sul d.d.l. A.S. 806 - Modifiche al codice di procedura penale in materia di sequestro di dispositivi e sistemi informatici, smartphone e memorie digitali: MURRO, *Prospettive in tema di sequestro dello smartphone: le novità approvate dal Senato*, in *Dir. pen. proc.*, 12/2024, 1619 ss.