PASQUALE RAUCCI

Le condizioni per l'accesso ai dati del cellulare per il diritto europeo

La Corte di Giustizia dell'Unione europea ha stabilito le condizioni in base alle quali la disciplina nazionale possa ritenersi conforme agli standard europei in tema di accesso ai dati del cellulare ad opera delle autorità inquirenti. In specie, la Corte ha stabilito che una normativa nazionale possa essere ritenuta conforme alla direttiva 2016/680 qualora definisca in maniera precisa i reati presupposto, disponga un previo controllo giurisdizionale rispetto all'accesso ai dati e garantisca l'utilizzo del criterio di "proporzionalità". Inoltre, è necessario informare la persona interessata dei motivi su cui si fonda l'autorizzazione ad accedere a tali dati, affinché egli possa eventualmente esercitare il suo diritto ad un ricorso effettivo.
La pronunzia si inserisce nel solco delle discussioni in tema di prova digitale, contribuendo ad offrire nuovi stimoli di riflessione sulla necessaria rivisitazione dell'odierno strumentario giuridico-processuale, ampliando lo spettro di analisi a valori estremamente ampi (la tutela della privacy) da bilanciare con l'interesse statuale alla prevenzione e repressione dei reati, evidenziando (probabilmente) sempre più le inadeguatezze dei vigenti strumenti di indagine in tema di formazione ed acquisizione della prova digitale.

The conditions for access to mobile data under European law

The Court of Justice of the European Union has established the conditions under which national legislation can be considered compliant with European standards regarding access to mobile phone data by investigating authorities. Specifically, the Court has established that national legislation can be considered compliant with Directive 2016/680 if it precisely defines the underlying crimes, provides for prior judicial review of access to data and guarantees the use of the "proportionality" criterion. Furthermore, it is necessary to inform the data subject of the reasons on which the authorization to access such data is based, so that he or she can possibly exercise his or her right to an effective remedy. The ruling falls within the framework of discussions on the subject of digital evidence, contributing to providing new stimuli for reflection on the necessary review of today's legal-procedural tools, broadening the spectrum of analysis to extremely broad values (the protection of privacy) to be balanced with the state interest in the prevention and repression of crimes, highlighting (probably) increasingly the inadequacies of the current investigative tools in terms of the formation and acquisition of digital evidence.

1. *Sintesi della decisione.* Con la sentenza resa dalla Grande sezione della Corte di giustizia dell'Unione europea il 04/10/2024, proc. C-548/21[1], si stabiliscono le condizioni in base alle quali la disciplina nazionale possa ritenersi conforme

[1] Rinvenibile con sintesi anche in *Arch. pen. web*, sezione Giurisprudenza europea, a cura di MONTAGNA, al link https://archiviopenale.it/corte-di-giustizia-dell-unione-europea-(grande-camera)-4-ottobre-2024-causa-c-548-21/contenuti/29682

agli *standard* europei in tema di trattamento dei dati personali ad opera delle autorità competenti, che ne siano entrati in possesso per fini di prevenzione, indagine, accertamento o perseguimento di reati e alla libera circolazione degli stessi.

Alla Corte del Lussemburgo, in effetti, è stata sottoposta una domanda di pronuncia pregiudiziale[2], ai sensi dell'art. 267 TFUE, dal Landesverwaltungsgericht Tirol (Tribunale amministrativo regionale del Tirolo, Austria) nell'ambito di una controversia tra C.G. e la Bezirkshauptmannschaft Landeck (autorità amministrativa del distretto di Landeck, Austria) in merito al sequestro del telefono cellulare di C.G. da parte delle autorità di polizia e ai tentativi di quest'ultima, nell'ambito di un'indagine sul traffico di droga, di sbloccare il telefono per accedere ai dati in esso contenuti.

In relazione a tale situazione, sono state sottoposte alla Corte le seguenti questioni pregiudiziali:

1) Se l'articolo 15, par. 1 (eventualmente in combinato disposto con l'articolo 5) della direttiva 2002/58[3], come modificata dalla direttiva 2009/136/CE[4], letto alla luce degli artt. 7 e 8 della Carta dei diritti fondamentali, debba essere interpretato nel senso che l'accesso delle autorità pubbliche ai dati conservati nei telefoni cellulari comporti un'ingerenza nei diritti fondamentali sanciti da detti articoli della Carta, che presenta una gravità tale che il suddetto accesso debba essere limitato, in materia di prevenzione, ricerca, accertamento e perseguimento dei reati, alla lotta contro la criminalità grave;

2) se l'art. 15, par. 1 della direttiva 2002/58, come modificata dalla direttiva 2009/136, letto alla luce degli artt. 7, 8 e 11 nonché dell'art. 52, par. 1, della Carta dei diritti fondamentali, debba essere interpretato nel senso che osti ad una normativa nazionale (quale l'art. 18 in combinato disposto con l'art. 99, par. 1, del codice di procedura penale austriaco), in forza della quale le autorità

---

[2] Domanda di pronuncia pregiudiziale proposta dal Landesverwaltungsgericht Tirol (Austria) il 6 settembre 2021, C.G. / Bezirkshauptmannschaft Landeck, C-548/21, ECLI:EU:C:2024:830.

[3] 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 (GU 2002, L 201, pag. 37).

[4] Direttiva 2009/136/CE del Parlamento europeo e del Consiglio del 25 novembre 2009 recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori (GU 2009, L 337, pag. 11).

preposte alla sicurezza si procurano autonomamente, nel corso di un'indagine penale, un accesso completo e non controllato a tutti i dati digitali conservati in un telefono cellulare, senza l'autorizzazione di un giudice o di un'entità amministrativa indipendente;
3) se l'art. 47 della Carta, eventualmente in combinato disposto con gli artt. 41 e 52 della Carta dei diritti fondamentali, sotto il profilo della parità delle armi e sotto il profilo di un mezzo di ricorso effettivo, debba essere inteso nel senso che osti ad una normativa di uno Stato membro (quale l'art. 18 in combinato disposto con l'art. 99, par. 1, del codice di procedura penale austriaco), la quale consenta di analizzare digitalmente un telefono cellulare.
L'11 novembre 2021, il giudice nazionale, in risposta alla richiesta della Corte del 20 ottobre 2021, ha affermato che nel caso di specie dovevano altresì essere rispettate le norme di cui alla direttiva 2016/680[5].
La domanda di pronuncia pregiudiziale sottoposta alla Corte, dunque, aveva ad oggetto l'interpretazione degli artt. 5 e 15, par. 1, della 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, come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, letta alla luce degli artt. 7, 8, 11, 41 e 47 e dell'art. 52, par. 1, della Carta dei diritti fondamentali dell'Unione europea. Tuttavia a seguito della riqualificazione dei fatti operata dalla Corte stessa, la normativa più pertinente oggetto di applicazione al caso di specie è stata individuata solo ed esclusivamente in quella di cui alla direttiva 680/2016.
Pertanto, con la prima e la seconda questione, come riqualificata, il giudice del rinvio ha chiesto in sostanza se l'articolo 4, par. 1, lett. c), della direttiva 2016/680, letto alla luce degli artt. 7 e 8 e dell'art. 52, par. 1, della Carta, osti a una normativa nazionale che conceda alle autorità competenti la possibilità di accedere ai dati contenuti in un telefono cellulare ai fini della prevenzione, dell'indagine, dell'accertamento e del perseguimento dei reati in generale e che non subordini l'esercizio di tale possibilità al controllo preventivo di un giudice o di un organo amministrativo indipendente.
Sulla scorta di quanto si andrà ad analizzare nel prosieguo, in risposta a tali

[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.

quesiti, la Corte ha stabilito che l'art. 4, par. 1, lett. c), della direttiva 2016/680, letto alla luce degli artt. 7 e 8 e dell'art. 52, par. 1, della Carta, debba essere interpretato nel senso che esso non osta a una normativa nazionale che conceda alle autorità competenti la possibilità di accedere ai dati contenuti in un telefono cellulare, ai fini della prevenzione, dell'indagine, dell'accertamento e del perseguimento dei reati in generale, se questa normativa:
a) definisce in modo sufficientemente preciso la natura o le categorie di reati in questione;
b) garantisce il rispetto del principio di proporzionalità;
c) fa sì che l'esercizio di questa possibilità, tranne in casi di urgenza debitamente giustificati, sia soggetto a un controllo preventivo da parte di un giudice o di un organo amministrativo indipendente[6].
Con la terza questione, poi, il giudice del rinvio intende essenzialmente stabilire se C.G. avrebbe dovuto essere informato dei tentativi di accesso ai dati contenuti nel suo telefono cellulare per poter esercitare il suo diritto a un ricorso effettivo garantito dall'art. 47 della Carta.
Rispetto a tale ultimo quesito, la Corte ha affermato che gli artt. 13 e 54 della direttiva 2016/680, letti alla luce degli artt. 47 e 52, par. 1, della Carta dei diritti fondamentali, devono essere interpretati nel senso che ostano a una normativa nazionale che autorizzi le autorità competenti a tentare di accedere ai dati contenuti in un telefono cellulare senza informare la persona interessata dei motivi su cui si fonda l'autorizzazione ad accedere a tali dati, rilasciata da un organo giurisdizionale o da un'autorità amministrativa indipendente, a partire dal momento in cui la comunicazione di tali informazioni non è più idonea a compromettere i compiti che incombono a tali autorità in forza di tale direttiva[7].

2. *La normativa europea oggetto di analisi:* iura novit curia. Il *focus* della pronunzia attiene alla verifica della compatibilità della legislazione nazionale (austriaca) alla direttiva (UE) 2016/680, del Parlamento europeo e del Consiglio, del 27 aprile 2016, in tema di accesso, per fini di indagine penale, ai dati contenuti nel telefono cellulare di un soggetto sottoposto alle indagini penali.
Sebbene il giudice nazionale abbia originariamente fatto riferimento alla direttiva 2002/58 e solo successivamente abbia affermato la rilevanza anche della poc'anzi menzionata direttiva del 2016, la Corte ha comunque ritenuto di poter vagliare la compatibilità della normativa nazionale con tale ultima direttiva,

[6] Corte giust. UE, Grande sezione, 04 ottobre 2024, C-548/21, 110.
[7] Ibidem, 123.

ritenuta quella pertinente al caso sottoposto, in quanto, come anche già affermato in precedenti pronunzie[8], qualora gli Stati membri attuino direttamente misure che derogano alla riservatezza delle comunicazioni elettroniche senza imporre obblighi di trattamento ai fornitori di tali comunicazioni, la protezione dei dati degli interessati non è disciplinata dalla direttiva 2002/58 ma unicamente dal diritto nazionale, fatta salva l'applicazione della direttiva 2016/680.
La Corte, dunque, conferma ancora una volta l'adesione all'aforisma *iura novit curia*[9], ritenuto all'evidenza la migliore espressione del principio di cooperazione tra i giudici nazionali e la Corte, come risultante dall'art. 267 TFUE, in forza del quale spetta alla Corte fornire al giudice nazionale una risposta utile che gli consenta di decidere la controversia di cui è investito, così se del caso riformulando le questioni ad essa sottoposte e prendendo in considerazione norme di diritto dell'Unione alle quali il giudice nazionale non abbia fatto riferimento nella formulazione delle sue questioni[10].
A tale riguardo, spetta alla Corte estrarre dall'insieme degli elementi forniti dal giudice nazionale, e in particolare dalla motivazione dell'ordinanza di rinvio, gli elementi del diritto dell'Unione che richiedono un'interpretazione alla luce dell'oggetto della controversia[11].

3. *L'estensione del perimetro della nozione di "trattamento dati": tentativo di accesso e «principio della limitazione delle finalità».* Nella pronunzia in esame, la Corte si pone innanzitutto il problema di verificare se la nozione di "trattamento" dei dati, di cui all'art. 3, par. 2 della direttiva 2016/680, in relazione all'ambito di applicazione della medesima fonte ed alle sue finalità, sia suscettibile di ricomprendere nel suo significato non solo la effettiva gestione del "dato", bensì anche il solo "tentativo" di entrarne in possesso.

---

[8] Corte giust. UE, 6 ottobre 2020, C-623/17, Privacy International EU:C:2020:790, 48; Corte giust. UE, 6 ottobre 2020, C-511/18, C-512/18 e C-520/18, La Quadrature du Net e.a., EU:C:2020:791, 103; Corte giust. UE, C-548/21, cit., 57.

[9] Brocardo che esprime la regola in base alla quale, anche nei processi ispirati al principio dispositivo (in virtù del quale la pronuncia giurisdizionale incontra limiti corrispondenti alle richieste avanzate dalle parti ed alle prove da esse prodotte o richieste), il giudice ha il potere-dovere di individuare, anche di sua iniziativa, e di applicare ai fatti dedotti ed accertati le norme giuridiche che, secondo il diritto vigente ed in base alle regole sull'efficacia della legge nello spazio e nel tempo, debbano disciplinare i fatti stessi, così Pizzorusso, *voce Iura novit curia, I) Ordinamento italiano*, in *Enc. giur.*, XVIII, 1.

[10] Corte giust. UE, 15 luglio 2021, C-742/19, Ministrstvo za obrambo, EU:C:2021:597, 31 e giurisprudenza citata; Corte giust. UE, 18 giugno 2024, C-352/22, Generalstaatsanwaltschaft Hamm (Richiesta di estradizione di un rifugiato in Turchia), EU:C:2024:521, 47; Corte giust. UE, C-548/21, cit., 60.

[11] Corte giust. UE, 22 giugno 2022, C-267/20, Volvo e DAF Trucks, EU:C:2022:494, 28 e giurisprudenza ivi citata; Corte giust. UE, C-548/21, cit., 61 e 64.

Pertanto, al fine di risolvere la questione, passa all'analisi letterale dell'art. 3, par. 2, della direttiva 2016/680[12], evidenziando come la norma, mediante l'uso delle espressioni «qualsiasi operazione», «qualsiasi insieme di operazioni» e qualsiasi «altro modo» intenda conferire un'ampia portata al concetto di messa a disposizione». Si è ritenuto, allora, che tali elementi testuali militino a favore di un'interpretazione estensiva del concetto di "trattamento", per cui allorquando le autorità di polizia sequestrano un telefono e lo manipolano al fine di estrarre e consultare i dati personali in esso contenuti, iniziano un trattamento ai sensi dell'art. 3, par. 2, della direttiva 2016/680, anche se poi tali autorità non saranno in grado, per motivi tecnici, di accedere a tali dati.
Tale interpretazione estensiva viene confermata dal disposto dell'art. 4, par. 1, lett. b), della direttiva 2016/680, ai sensi del quale gli Stati membri devono garantire che i dati personali siano raccolti per finalità determinate, esplicite e legittime, e non siano trattati in modo incompatibile con esse. Con tale norma, dunque, si sancisce il «principio della limitazione delle finalità»[13], da cui è possibile ricavare il corollario secondo cui la finalità stessa della raccolta deve essere determinata già nella fase in cui le autorità competenti tentano di accedere ai dati personali, in quanto tale attività consentirebbe loro di raccogliere, estrarre o consultare immediatamente i dati in questione.
Per tale via, allora, si riuscirebbe a garantire un "livello elevato di protezione dei dati personali delle persone fisiche", ciò che alla luce dei «Considerando 4, 7 e 15» costituisce uno degli obiettivi della direttiva 2016/680.
Solo siffatta interpretazione, inoltre, riuscirebbe ad essere coerente con il «principio della certezza del diritto» che, secondo la costante giurisprudenza della Corte, richiede che l'applicazione delle norme di legge sia prevedibile da parte dei singoli, necessità ancor più sentita qualora tali norme possano avere conseguenze negative[14]. Invero, ragionando *a contrario*, un'interpretazione secondo la quale l'applicabilità della direttiva 2016/680 dipenderebbe dal successo del tentativo di accesso ai dati personali contenuti in un telefono cellulare creerebbe incertezza sulla disciplina giuridica applicabile sia per le autorità nazionali competenti sia per le parti in causa, situazione che risulterebbe

---

12 In cui si definisce il "trattamento" come "qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati su dati personali o insiemi di dati personali, come l'estrazione, la consultazione, la diffusione o la messa a disposizione in altro modo".

13 Cfr., in tal senso, Corte giust. UE, 23 gennaio 2023, C-205/21 Ministerstvo na vatreshnite raboti (Registrazione di dati biometrici e genetici da parte della polizia) EU:C:2023:49, 122.

14 Corte giust. UE, 27 giugno 2024, C-148/23, Gestore dei Servizi Energetici, EU:C:2024:555, 42, nonché v. anche giurispruenza citata.

incompatibile con il basilare principio, suddetto, di certezza del diritto.
L'effetto utile della direttiva 2016/680 dovrebbe allora privilegiare un'interpretazione del suo oggetto che non si limiti al trattamento dei dati in senso stretto, ma che si estenda anche al tentativo di accedere ai dati di cui si intende effettuare il trattamento[15].
Tale esegesi, inoltre, risulta essere in linea con la giurisprudenza della Corte europea dei diritti dell'uomo, la quale, in una recente pronuncia[16], ha affermato che in tema di archiviazione della messaggistica elettronica - rientrante nel perimetro di applicazione dell'art. 8 C.E.D.U - ed a prescindere dall'effettiva acquisizione di tali dati, costituisce una grave ingerenza nella sfera privata e individuale la sola esistenza di un obbligo *ex lege* di consentirne l'accesso. In tale pronunzia, dopo aver ribadito la centralità del diritto alla riservatezza, i Giudici di Strasburgo evidenziano la necessità che le norme in materia di conservazione, acquisizione e trattamento automatizzato dei dati esterni alle conversazioni (*traffic data*) e del loro contenuto (*content data*) assicurino adeguate garanzie procedurali contro i possibili abusi, limitando l'archiviazione a finalità predeterminate e prevedendo un periodo di conservazione «non superiore al necessario»[17].
La nozione di "trattamento dei dati", dunque, si espande a quella di "tentativo di trattamento", così attraendo a sé ogni attività - dell'uomo o automatizzata - tale da incidere anche solo in via possibilistica sul trattamento medesimo. La problematica, a questo punto, arretra al concetto stesso di "tentativo", perché occorre stabilire l'esatta portata del termine. Si vuol dire che, a questo punto, sarà necessario individuare i confini esatti della suddetta nozione in quanto ai fini dell'applicazione della direttiva 680/2016 è indispensabile capire quale azione sia suscettibile di integrare gli estremi del "tentativo di trattamento", anche tenuto conto del fatto che potrebbe entrare in gioco l'aspetto soggettivo del soggetto agente[18].

4. *«Proporzionalità» e «minimizzazione dei dati»: i principi legittimanti la restrizione dei diritti fondamentali.* Stabilita l'estensione del concetto di "trattamento", la Corte sposta la sua attenzione sui principi di diritto che trovano applicazione

[15] Considerazioni dell'Avvocato Generale, Corte giust. UE, C-548/21, cit., 53.
[16] Corte EDU, 11 gennaio 2022, Ekimdzhiev e altri c. Bulgaria, 372.
[17] Così ERTOLA, *Conservazione e acquisizione di comunicazioni criptate*, in *Riv. it. dir. proc. pen.*, 2, 1 giugno 2024, 850.
[18] Sul concetto di «tentativo», non solo in ambito penalistico ma anche per uno studio storico, cfr. LAMBERTINI, *voce Tentativo*, in *Enc. dir.*, XLIV, 1992, 93 e ss.

nel caso in cui un'Autorità giudiziaria intenda procedere al trattamento dei dati di un soggetto per fini investigativi e/o repressione di reati. Ciò che v'è da stabilire, dunque, sono i parametri che devono guidare l'interprete nel procedere ad estendere o comprimere le diverse esigenze meritevoli di tutela, ovvero: l'interesse privato alla tutela dei propri dati o quello pubblicistico alla repressione dei fenomeni criminosi.

A tal uopo, il principio di "proporzionalità" è quello legalmente eletto[19].

L'origine e l'elaborazione di tale principio in sede sovranazionale è individuabile, da un lato, per come è stato recepito dal diritto giurisprudenziale, sino a divenire un sovra-principio, vale a dire un punto fondante a base della intera costruzione giuridica dell'Unione, e un meta-principio, ossia una chiave di lettura e di applicazione degli altri diritti fondamentali riconosciuti dal sistema europeo. Dall'altro, il Trattato di Lisbona ha, da ultimo, consacrato nel diritto positivo, al suo rango più alto, il medesimo principio, così recependo la elaborazione operatane dalla Corte di giustizia[20].

Espressioni del "principio di proporzionalità" si rinvengono ai parr. 3 e 4 dell'art. 5 TUE, nonché agli artt. 49, par. 3, e 52 par. 1, della C.D.F.U.E., quest'ultima elevata, in forza dell'art. 6 TUE, a fonte primaria dell'Unione, al pari dei Trattati.

La cogenza di tale principio è rinvenibile in una recente sentenza della Grande sezione della Corte di giustizia[21], in ambito penale sostanziale, ove si è affermato il principio secondo cui il criterio di proporzionalità della sanzione – stabilito da singole direttive, ovvero fondato sull'art. 49, par. 3, della Carta – è dotato di

[19] Per un approfondimento del principio in parola rispetto alla fase delle indagini in ambito interno e per le origini europee, cfr. BELVINI, *Principio di proporzionalità e attività investigativa*, Napoli, 2022.

[20] Così CAIANIELLO, *Il principio di proporzionalità nel procedimento penale*, in *Dir. pen. cont.*, Riv. trim. 3-4, 2014, 148-149; ed *ivi* in nota 24, ove chiarisce che il primo riferimento, secondo la dottrina in materia, è fatto risalire al 1956 a seguito della pronunzia della Corte giust. UE, 29 novembre 1956, C-8/55, Fédération Charbonnière de Belgique c. Alta autorità, nella cui motivazione si osserva che ogni reazione dovrebbe sempre «risultare commisurata all'importanza dell'atto illecito». Da allora, attraverso uno sviluppo continuo sino ad oggi, la proporzionalità è stata progressivamente saldata con i diritti fondamentali, quali "categorie propriamente costituzionali del diritto comunitario e quali strumenti di legittimazione della sua autonomia e preminenza sui diritti nazionali" (in tal senso MARLETTA, *Il principio di proporzionalità nella disciplina del mandato d'arresto europeo,* tesi dottorale, Bologna, 2013, 80. A questo recente lavoro si rinvia per una ampia analisi del principio di proporzionalità nella elaborazione dell'Unione europea, e sui suoi riflessi in ambito di cooperazione giudiziaria in materia penale). Afferma TRIDIMAS, *The General principles of EU Law*, in *Oxford University Press*, 2006, 194: "In fact, this public law element of proportionality has become much more prevalent in recent years as the ECJ has intensified judicial review of national measures on grounds of compatibility with human rights. The Court appears to engage in what can be termed collateral rewiew on grounds of proportionality".

[21] Corte giust. UE, Grande sezione, 8 marzo 2022, C-205/20, NE, ECLI:EU:C:2022:168.

effetto diretto nell'ordinamento degli Stati membri. Con la cruciale conseguenza che il giudice penale, nell'ambito di applicazione del diritto dell'Unione, sarà tenuto a disapplicare discipline legislative nazionali contrastanti, seppur «nei soli limiti necessari per consentire l'irrogazione di sanzioni proporzionate». Il tema del principio di proporzionalità rispetto alla direttiva 2016/680 rileva nella misura in cui tale fonte europea ha riguardo soltanto al trattamento di dati da parte delle autorità competenti a fini di prevenzione, indagine accertamento e perseguimento di tutti i tipi di reato, senza stabilire limiti fondati sulla gravità dei reati, sicché, in assenza di qualsiasi indicazione di tal fatta, si pone un problema di possibile non uniforme applicazione di tale direttiva da parte degli Stati membri, potendo le valutazioni di ciascun ordinamento nazionale (sulla maggiore o minore gravità di una condotta punibile) differire notevolmente[22]. Pertanto, facendo applicazione del principio di proporzionalità, la Corte ha ricavato il cd. "principio della minimizzazione dei dati", sulla scorta del quale ha ritenuto che (ai sensi dell'art. 4, par. 1, lett. c), della direttiva 2016/680) gli Stati membri devono garantire che i dati personali siano «adeguati, pertinenti e non eccessivi rispetto alle finalità per le quali sono trattati»[23]. Ne consegue che la raccolta di dati personali nell'ambito di un procedimento penale e la loro conservazione da parte delle autorità di polizia per le finalità di cui all'art. 1, par. 1 di tale direttiva devono, come qualsiasi trattamento rientrante nel suo ambito di applicazione, rispettare tale principio[24].

4.1. *Pre-condizioni al giudizio di proporzionalità: norme chiare e sindacato giurisdizionale.* Dovendosi fare applicazione del principio di proporzionalità, declinato nella sua specie di "minimizzazione dei dati", si impone un giudizio di bilanciamento tra le contrapposte esigenze della prevenzione, indagine, accertamento e del perseguimento dei reati in generale, con quelle di tutela delle libertà fondamentali.

4.2. *Proporzionalità e tutela dei diritti fondamentali.* La Corte pertanto per la

[22] Cfr. le osservazioni degli intervenienti al giudizio dinanzi la Corte giust. UE, C-548/21, cit. In specie, il governo francese cita come esempio i reati in materia di detenzione e traffico di stupefacenti, sulla cui gravità le norme penali dell'Austria e della Francia differiscono. Il governo svedese si pronuncia in senso analogo.

[23] Corte giust. UE, 30 gennaio 2024, C-118/22, Direktor na Glavna direktsia "Natsionalna politsia" pri MVR - Sofia, EU:C:2024:97, 41, ed ivi per la giurisprudenza citata.

[24] Ibidem, 42 ed ivi per la giurisprudenza citata.

disamina della questione passa in rassegna la direttiva, rilevando *in primis* come la finalità di essa sia la contribuzione alla creazione di uno spazio di libertà, sicurezza e giustizia all'interno dell'Unione[25]. In tale ottica, l'obiettivo di garantire un livello elevato di protezione dei dati personali delle persone fisiche, come sottolineato nel "Considerando 104", deve tenere conto delle restrizioni che tale direttiva consente di apportare a tale diritto previsto dall'art. 8 della Carta dei diritti fondamentali, e al diritto al rispetto della vita privata e familiare, tutelato dal precedente art. 7. Sicché tali ultimi devono essere interpretati conformemente ai requisiti di cui all'art. 52, n. 1, tra i quali figura il rispetto proprio del principio di proporzionalità[26].

In effetti, la Corte di giustizia specifica come tali diritti non siano prerogative assolute, ma devono essere considerati in relazione alla loro funzione nella società e bilanciati con altri diritti di pari livello. Pertanto, la Corte arriva ad affermare che intanto le restrizioni a tali diritti fondamentali possono essere imposte in quanto esse siano ritenute "necessarie"[27] e rispondono effettivamente a "obiettivi di interesse generale"[28] riconosciuti dall'Unione o alla "necessità di proteggere i diritti e le libertà altrui".

La normativa deputata a stabilire siffatte restrizioni, poi, deve stabilire «norme chiare e precise» e rientrare nei limiti dello «stretto necessario»[29].

---

25 Come emerge dai considerando 2 e 4 della direttiva 2016/680, e ciò pur istituendo un quadro solido e coerente per la protezione dei dati personali al fine di garantire il rispetto del diritto fondamentale di tutela delle persone fisiche con riguardo al trattamento dei dati personali che le riguardano, riconosciuto dall'art. 8, par. 1della Carta e dall'art. 16, par. 1 del TFUE. Cfr., in tal senso, Corte giust. UE, 25 febbraio 2021, Commissione/Spagna, C-658/19, EU:C:2021:138, 75; Corte giust. UE, C-548/21, cit., 82.

26 Cfr., in tal senso, sentenza del Tribunale di primo grado U. E., C-118/22, Direktor na Glavna direktsia "Natsionalna politsia" pri MVR - Sofia, EU:C:2024:97, 33; Corte giust. UE, C-548/21, cit., 84.

27 Sulla "necessarietà", dice la Corte, tale requisito non è soddisfatto qualora l'obiettivo di interesse generale perseguito possa ragionevolmente essere raggiunto in modo altrettanto efficace con altri mezzi meno pregiudizievoli per i diritti fondamentali degli interessati (v., in tal senso Corte giust. UE, C-118/22, cit., 40 ed ivi per la giurisprudenza citata); al contrario, il requisito della necessità è soddisfatto quando l'obiettivo perseguito dal trattamento dei dati in questione non può ragionevolmente essere raggiunto con pari efficacia con altri mezzi meno invasivi dei diritti fondamentali degli interessati, Corte giust. UE, C-548/21, cit., 87 e 88.

28 Per tale requisito, dice la Corte, occorre sottolineare che il trattamento di dati personali nell'ambito di un'indagine di polizia finalizzata al perseguimento di un reato, quale il tentativo di accedere ai dati contenuti in un telefono cellulare, deve essere considerato, in linea di principio, come effettivamente rispondente a un obiettivo di interesse generale riconosciuto dall'Unione, ai sensi dell'art. 52, par. 1 della Carta; Corte giust. UE, C-548/21, cit., 86.

29 Corte giust. UE, Grande sezione, 30 gennaio 2024, C-118/22, NG, ECLI:EU:C:2024:97, 39 ed ivi per la giurisprudenza citata; Corte giust. UE, C-548/21, cit., 85.

Ciò posto, considerato che il canone di proporzione si caratterizza, nel suo momento applicativo, per un'elevata flessibilità, tale in particolare da esaltare la componente argomentativa e persuasiva del metodo giuridico[30], si rende necessaria una esatta ponderazione di tutti i fattori pertinenti del caso[31].
Nella specie, gli elementi da valutare includono: ***i)*** la gravità della restrizione così imposta all'esercizio dei diritti fondamentali in questione, che dipende dalla natura e dalla sensibilità dei dati a cui le autorità di polizia possono avere accesso; ***ii)*** l'importanza dell'obiettivo di interesse pubblico perseguito dalla restrizione; ***iii)*** il legame tra il proprietario del dispositivo elettronico ed il reato per cui si procede e la rilevanza dei dati in questione per l'accertamento dei fatti.

4.3. *Proporzionalità e finalità di prevenzione, indagine, accertamento e perseguimento di reati.* Tanto considerato in tema di tutela dei diritti fondamentali, la Corte procede al vaglio dell'importanza dell'obiettivo perseguito dalla direttiva medesima, al fine di verificare - mediante il predetto criterio di proporzionalità - a quali condizioni tali diritti possano essere sacrificati.
In primis, dunque, si afferma che la «gravità del reato» oggetto di indagine è certamente uno dei parametri centrali per esaminare la proporzionalità della grave ingerenza costituita dall'accesso ai dati personali contenuti in un telefono cellulare.
Tuttavia, limitare l'accesso ai dati contenuti in un telefono cellulare solo alla lotta contro i reati gravi, circoscriverebbe in maniera eccessiva i poteri investigativi delle autorità competenti, così aumentando il rischio di impunità.
Orbene, tenuto conto del fatto che le esigenze investigative devono essere salvaguardate e che ai sensi dell'art. 52, par. 1, della Carta ogni limitazione ad un diritto fondamentale deve essere prevista da una «base giuridica» sufficientemente chiara e precisa[32], la Corte giunge ad affermare che spetta al legislatore nazionale definire con sufficiente precisione i fattori da prendere in considerazione, in particolare la natura o le categorie dei reati in questione[33].
Aggiungasi che al fine di garantire che il principio di proporzionalità sia rispettato in ogni caso specifico attraverso la ponderazione di tutti i fattori pertinenti, è essenziale che, qualora l'accesso ai dati personali da parte delle autorità

[30] CAIANIELLO, *Il principio di proporzionalità*, cit., 144.
[31] Corte giust. UE, C-118/22, cit., 62 e 63 ed ivi per la giurisprudenza citata.
[32] Si veda, a tal proposito, Corte giust. UE, C-205/21, cit., 65, ed ivi per la giurisprudenza citata.
[33] Corte giust. UE, C-548/21, cit., 99.

nazionali competenti comporti il rischio di un'interferenza grave, o addirittura particolarmente grave, con i diritti fondamentali della persona interessata, tale accesso sia soggetto a un controllo preventivo da parte di un Tribunale o di un organo amministrativo indipendente[34].
Per quanto riguarda le indagini penali, tale controllo richiede che il Tribunale o l'organismo anzidetto sia in grado di garantire un giusto equilibrio tra gli interessi legittimi legati alle esigenze dell'indagine nell'ambito della lotta contro il crimine, da un lato, e i diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali delle persone i cui dati sono interessati dall'accesso, dall'altro.
Tale organo, allora deve garantire i requisiti della "terzietà" ed "imparzialità". Nei primi commenti della dottrina, dunque, si è fatto ben presto riferimento al requisito della «doppia riserva di legge e di giurisdizione»[35], proprio perché (quanto al secondo requisito in particolare), in materia processuale penale è solo il giudice, il soggetto legittimato ad incidere su una libertà fondamentale[36].
La Corte ritiene che il menzionato "controllo indipendente" debba avvenire prima di qualsiasi tentativo di accesso ai dati in questione, tranne in un caso di urgenza debitamente giustificato, nel qual caso tale controllo deve avvenire senza indugio. Un controllo solo successivo, precisa la Corte, non servirebbe allo scopo di impedire l'autorizzazione di un accesso ai dati in questione che superi i limiti dello stretto necessario[37].

5. La decisione alla prima e seconda questione pregiudiziale. Sulla scorta di tali argomentazioni, si giunge così a ritenere, in risposta alla prima e alla seconda questione, che l'art. 4, par. 1, lett. c), della direttiva 2016/680, letto alla luce degli artt. 7 e 8 nonchè dell'art. 52, par. 1, della Carta, deve essere interpretato nel senso che esso non osta a una normativa nazionale che conceda alle autorità competenti la possibilità di accedere ai dati contenuti in un telefono cellulare, ai fini della prevenzione, dell'indagine, dell'accertamento e del perseguimento dei reati in generale, se questo regolamento:

---

[34] Ibidem, 102.
[35] FILIPPI, *La CGUE mette i paletti all'accesso ai dati del cellulare*, cit.
[36] *Ibidem*, il quale poi suggerisce che «Il legislatore italiano dovrà perciò provvedere in tal senso e potrebbe indicare gli stessi reati che oggi consentono l'intercettazione di comunicazioni e il medesimo procedimento autorizzativo». Inoltre, sulla necessità del previsto controllo giurisdizionale, conformemente a precedenti pronunzie già rese dalla Corte di Giustizia UE, si è espresso DINACCI, *I modi acquisitivi della messaggistica chat o e-mail: verso letture rispettose dei principi*, in *questa Riv.*, 2024, 1.
[37] Corte giust. UE, C-548/21, cit., 104.

a) definisce in modo sufficientemente preciso la natura o le categorie di reati in questione,
b) garantisce il rispetto del principio di proporzionalità, e
c) fa sì che l'esercizio di questa possibilità, tranne in casi di urgenza debitamente giustificati, sia soggetto a un controllo preventivo da parte di un giudice o di un organo amministrativo indipendente.

6. *Obblighi informativi e diritto ad un ricorso effettivo.* La Corte, così, passa all'analisi della terza questione pregiudiziale sottopostale, ovvero, in sostanza, del quesito se gli artt. 13[38] e 54[39] della direttiva 2016/680, letti alla luce degli artt.

[38] Art. 13, rubricato «Informazioni da rendere disponibili o da fornire all'interessato», prevede: «1. Gli Stati membri dispongono che il titolare del trattamento metta a disposizione dell'interessato almeno le seguenti informazioni:
a) l'identità e i dati di contatto del titolare del trattamento;
b) i dati di contatto del responsabile della protezione dei dati, se del caso;
c) le finalità del trattamento cui sono destinati i dati personali;
d) il diritto di proporre reclamo a un'autorità di controllo e i dati di contatto di detta autorità;
e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati e la rettifica o la cancellazione dei dati personali e la limitazione del trattamento dei dati personali che lo riguardano.
2. In aggiunta alle informazioni di cui al paragrafo 1, gli Stati membri dispongono per legge che il titolare del trattamento fornisca all'interessato, in casi specifici, le seguenti ulteriori informazioni per consentire l'esercizio dei diritti dell'interessato:
a) la base giuridica per il trattamento;
b) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
c) se del caso, le categorie di destinatari dei dati personali, anche in paesi terzi o in seno a organizzazioni internazionali;
d) se necessario, ulteriori informazioni, in particolare nel caso in cui i dati personali siano raccolti all'insaputa dell'interessato.
3. Gli Stati membri possono adottare misure legislative intese a ritardare, limitare o escludere la comunicazione di informazioni all'interessato ai sensi del par. 2 nella misura e per il tempo in cui ciò costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata al fine di:
a) non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari;
b) non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali;
c) proteggere la sicurezza pubblica;
d) proteggere la sicurezza nazionale;
e) proteggere i diritti e le libertà altrui.
4. Gli Stati membri possono adottare misure legislative al fine di determinare le categorie di trattamenti cui può applicarsi, in tutto o in parte, una delle lettere del par. 3.

[39] Art. 54, rubricato «Diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento», prevede: «Gli Stati membri dispongono che, fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile, compreso il diritto di proporre reclamo a un'autorità

47 e 52, par. 1 della Carta, debbano essere interpretati nel senso che ostano a una normativa nazionale che consenta alle autorità competenti in materia penale di tentare di accedere ai dati contenuti in un telefono cellulare senza informare la persona interessata[40].

La Corte di giustizia, dunque, ritiene che spetti alle autorità nazionali competenti tanto informare le persone interessate dei motivi su cui si basa l'autorizzazione giurisdizionale all'accesso ai dati del cellulare (non appena ciò non possa compromettere le indagini svolte da tali autorità), quanto mettere a loro disposizione tutte le informazioni previste all'art. 13, par. 1 della direttiva 2016/680. Tali informazioni sono infatti necessarie per consentire, in particolare, l'esercizio del diritto di ricorso espressamente previsto dall'art. 54 della direttiva 2016/680[41].

La Corte di giustizia, così, si allinea alla giurisprudenza della Corte EDU resa proprio rispetto ad un caso italiano[42], ove si è ritenuto necessario - in tema di intercettazione di comunicazioni - che la legge nazionale preveda l'obbligo della successiva notifica al terzo interessato della misura di sorveglianza segreta allorquando tale adempimento sia possibile in concreto senza che l'informazione stessa comprometta lo scopo della sorveglianza, e che ciò possa costituire una condizione per l'accesso al rimedio giudiziario[43]. Anche i giudici di Strasburgo, in effetti, avevano evidenziato la necessità di predisporre strumenti giuridici a garanzia dei diritti inviolabili di chi non fosse direttamente coinvolto nelle indagini penali, in quanto non indiziati di essere coinvolti nel reato, nel caso in cui l'intercettazione di conversazioni o comunicazioni sia disposta nei loro confronti.

---

di controllo ai sensi dell'articolo 52, l'interessato abbia il diritto a un ricorso giurisdizionale effettivo qualora ritenga che i diritti di cui gode ai sensi delle disposizioni adottate a norma della presente direttiva siano stati violati a seguito del trattamento dei propri dati personali in violazione di tali disposizioni».

[40] Corte giust. UE, C-548/21, cit., 114.

[41] Cfr., in tal senso Corte giust. UE, 17 novembre 2022, C-350/21, Spetsializirana prokuratura EU:C:2022:896, 70 e 71 (sulla conservazione dei dati relativi al traffico e all'ubicazione), ed ivi per la giurisprudenza citata.

[42] Corte EDU, 23 maggio 2024, Contrada c. Italia.

[43] Così FILIPPI, *op. cit.*, nonché giurisprudenza ivi citata. L'A., invero, rileva come tale informazione non sia prevista dalla legge italiana in tema di intercettazione, tanto è vero che la Corte EDU ha condannato l'Italia per tale lacuna. Corte EDU, Grande camera, 4 dicembre 2015, R.Z. v. Russia; Corte EDU, 11 gennaio 2022, E. and others v. Bulgaria; in precedenza Corte EDU, 6 settembre 1978, K. e altri *v.* Germania, in cui era già stato osservato come la successiva notifica a ciascun interessato da una misura di sorveglianza segreta potrebbe mettere a repentaglio l'obiettivo a lungo termine che originariamente ha motivato il provvedimento e come l'interessato debba essere informato non appena la notifica possa essere effettuata senza compromettere lo scopo della restrizione.

7. Prime riflessioni sui possibili risvolti interni della pronunzia. La sentenza afferma in proposito alcuni importanti ed inediti principi di diritto che non potranno non essere attuati dalle legislazioni nazionali[44] e che offrono all'interprete vari spunti di riflessione.

E' interessante individuare in tale pronunzia questi snodi, incasellandosi essi in più ampi dibattiti interpretativi che nell'ultimo periodo stanno interessando tanto la dottrina quanto i Supremi consessi giurisprudenziali, nonché anche lo stesso legislatore nell'ambito della sua opera inventiva.

In effetti, è noto che il tema della digitalizzazione degli elementi di prova, ai fini del loro successivo utilizzo processuale, pone incessanti problematiche in continua evoluzione, in ragione di un inarrestabile sviluppo tecnologico[45]. Il tema dell'acquisizione ed utilizzazione dei dati digitali dai dispositivi elettronici, invero, nei nostri confini, ha dato luogo ad interessanti pronunzie tanto della Corte costituzionale (cfr. sent. 170 del 2023[46]) quanto della Corte di cassazione a Sezioni unite[47], risolvendo quesiti che però sembrano celare orizzonti problematici ben più distanti e ancora da esplorare[48]. Mentre, però, la questione sottoposta alla Consulta (nell'ambito di un conflitto di attribuzioni di poteri dello Stato) aveva per oggetto la verifica della estensione della tutela costituzionale del concetto di "comunicazione" [49] e quella delle sentenze gemelle sulla

---

[44] Così FILIPPI, *La CGUE mette i paletti all'accesso ai dati del cellulare*, in *Altalex*, 10/10/2024, reperibile al link https://www.altalex.com/documents/2024/10/10/cgue-mette-paletti-accesso-dati-cellulare

[45] Sul punto, per un approfondimento sul tema del rapporto tra il sequestro dei dispositivi informatici rispetto alla salvaguardia della legalità in tema di mezzi di ricerca della prova, si segnala DINACCI, *Sequestro di dispositivi informatici: imposizioni tecnologiche e scelte interpretative. Alla ricerca di un recupero della legalità probatoria*, in *questa Riv.*, 2025, 1.

[46] Corte cost., 7 giugno 2023, n. 170, in *Giur. cost.*, 4, 2023, con note di D'ANDREA (p. 1713) e CHELO, 1746 e ss., nel giudizio per conflitto di attribuzione tra poteri dello Stato.

[47] Cass., Sez. un., 14 giugno 2024, n.ri 23755 e 23756; per un primo commento, v. SPANGHER, *Criptofonini: le sentenze delle Sezioni Unite*, in giustiziainsieme.it, 20 giugno 2024; cfr. anche DANIELE, *La mappa del controllo giurisdizionale quando l'OEI ha ad oggetto prove già in possesso dell'autorità straniera*, in *sistemapenale.it*, 17/07/2024, reperibile al link https://www.sistemapenale.it/it/scheda/daniele-le-sentenze-gemelle-delle-sezioni-unite-sui-criptofonini#_ftn1

[48] Per un'analisi dell'evoluzione e l'involuzione delle problematiche riguardanti la materia delle intercettazioni telefoniche e telematiche analizzandone patologie, storture e nuovi approdi applicativi, suggerendo in conclusione un approccio europeisticamente orientato volto alla salvaguardia dei principi di eguaglianza, di proporzionalità e di legalità, cfr. GAITO, *Comunicazioni criptate ed esigenze difensive (da Blackberry a Sky-ECC)*, in *questa Riv.*, 2024, 1, editoriale.

[49] Sulle ricadute della sent. Corte cost. 170/23, nonché della Corte giust. UE, Grande sezione, 2 marzo 2021, H. K. c. Prokuratuur, ed in specie riguardo le problematiche normative ed interpretative sulle forme operative per l'acquisizione della messaggistica chat o e-mail, cfr. DINACCI, *I modi acquisitivi della*

questione Sky-ECC le condizioni legittimanti la circolazione della prova a livello transnazionale[50], quella in esame si caratterizza per un'estensione notevolmente maggiore. Invero, nella vicenda affrontata dalla Corte di giustizia le acquisizioni probatorie degli organi inquirenti devono confrontarsi con un fenomeno giuridico evidentemente superiore, ovvero l'accesso ed il trattamento ai dati personali del soggetto nel fuoco della tutela dei diritti fondamentali tra cui quello alla vita privata. Non solo, dunque, dati comunicativi ma ogni tipologia di dato. L'angolo prospettico dell'interprete, allora, sembra davvero allargarsi sino ai massimi estremi.

A livello sovranazionale, poi, tale pronunzia fa seguito alla decisione del 30 aprile 2024 con cui la Grande sezione della Corte di giustizia dell'Unione europea si è pronunciata in merito all'analoga vicenda dei messaggi criptati scambiati attraverso la piattaforma *Encrochat*[51] e, comunque, un ulteriore tassello al mosaico verrà aggiunto dalla Corte europea dei diritti dell'uomo[52], anch'essa chiamata ad esprimersi al riguardo[53].

Ebbene la presente pronunzia della Corte giust. UE si incanala in questi solchi, come detto, ancora del tutto da arare, rispetto ai quali però iniziano ad essere

---

messaggistica chat o e-mail, cit.

[50] DANIELE, *op. cit.*, più precisamente afferma che «La diatriba, come è ormai ben noto, concerne la natura e le conseguenti garanzie procedimentali applicabili all'acquisizione delle conversazioni via chat intercorse fra alcuni esponenti di associazioni criminali dedite al traffico di stupefacenti attraverso piattaforme online di tipo criptato, che avevano loro consentito di comunicare in modo riservato mediante smartphone appositamente modificati». In tema di comunicazioni mediante dispositivi criptati, e sugli strumenti giuridici applicati dalla giurisprudenza per la captazione di tali conversazioni, cfr. FURFARO, *Intercettazioni telefoniche – «Pin to pin» Blackberry*, in *questa Riv.*, 2016, 1.

51 Corte giust. UE, 30 aprile 2024, C-670/22, M.N.; Valentini, *Ultimissime*, in *Proc. pen. giust.*, reperibile al link https://www.processopenaleegiustizia.it/Tool/Evidenza/Single/view_html?id_evidenza=3169 rileva che con tale sentenza la Corte di Giustizia ha fornito alcune indicazioni sulla corretta interpretazione della direttiva 2014/41/UE, in forza della quale, ferma la necessità di tutelare i diritti dei soggetti sottoposti all'intercettazione (art. 31), il giudice nazionale è tenuto ad espungere ogni dato rispetto al quale la persona coinvolta nel procedimento non sia in grado di articolare efficacemente le proprie difese: se così non fosse, sulla valutazione dei fatti influirebbero informazioni ed elementi di prova acquisiti e valutati in un ambiente estraneo al contraddittorio e lesivo, perciò, delle prerogative processuali dell'accusato (art. 14, par. 7). Quindi, se nel processo in atto nello Stato di emissione, l'imputato non fosse in grado di misurarsi con i materiali raccolti tramite la collaborazione tra autorità inquirenti, quegli elementi sarebbero inutilizzabili (cfr. Corte giust. UE, 2 marzo 2021, C-746/18).

[52] Corte EDU, proc. n. 44715/20 (A.L c. Francia) e n. 47930/21 (E.J. c. Francia). Il 3 gennaio 2022 la Corte EDU ha sottoposto quesiti alle parti chiedendo, in particolare, se esse avessero avuto la possibilità di contestare le misure di intercettazione dinanzi ai giudici francesi competenti (ma non ne avessero fatto uso).

[53] Così DANIELE, *op. cit.*, riferendosi alle sentenze della Cass., Sez. un., 14 giugno 2024, n.ri 23755 e 23756.

fin troppo chiari due aspetti essenziali che riguardano il nostro ordinamento: la necessità di maggiore tutela dei diritti della persona e la necessità di approntare uno strumentario processuale adeguato alle continue evoluzioni tecnologiche[54], le quali - in specie nel momento investigativo - si stanno dimostrando sempre più intrusive della sfera personale dell'individuo.
E' proprio la consapevolezza della sempre maggiore "intrusività" del mezzo tecnologico adoperato che deve far riflettere sull'incidenza dello stesso rispetto alla (inevitabile) compressione dei diritti del soggetto.
Sul punto, è noto che - nel nostro sistema processuale - una volta eseguita una perquisizione e sequestro, le autorità inquirenti, mediante la cd. "copia forense", dispongono dell'intero contenuto del dispositivo in loro possesso[55]. Orbene, la Corte non manca di evidenziare[56] come tale accesso possa riguardare non solo i dati relativi al traffico e alla localizzazione, ma anche le fotografie e la cronologia di navigazione in Internet del telefono, e persino parte del contenuto delle comunicazioni effettuate con il telefono, in particolare i messaggi memorizzati su di esso. L'accesso completo ai dati del cellulare, allora, può certamente qualificarsi come "gravemente restrittivo" dei diritti fondamentali tutelati dalla direttiva 680/2016 UE in ragione del fatto che la loro consultazione può consentire di trarre conclusioni molto precise sulla vita privata dell'interessato (come, ad esempio: le sue abitudini quotidiane, i luoghi di residenza permanente o temporanea, gli spostamenti quotidiani o di altro tipo, le attività, le relazioni sociali e gli ambienti sociali frequentati dall'interessato).
Vieppiù, non si può escludere che i dati contenuti in un telefono cellulare possano includere dati particolarmente sensibili (quali ad es. quelli 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, biometrici o di dati relativi alla salute o alla vita sessuale della persona fisica o al suo

[54] Esigenza già segnalata da FURFARO, *Intercettazioni telefoniche – «Pin to pin» Blackberry*, cit., 1, il quale rilevava come l'esperienza giudiziaria dei decenni precedenti ha consentito di registrare, non soltanto la crescita esponenziale dell'utilizzazione di strumenti sempre più sofisticati per l'acquisizione di rilievi, tracce, notizie, comportamenti umani utili a fini di indagine e di prova, ma, attraverso l'interpretazione, il progressivo adattamento di istituti e precetti normativi a situazione che in comune tra loro hanno soltanto l'invasione degli spazi della vita privata e della comunicazione.

[55] Sugli indirizzi giurisprudenziali, tesi ad evitare che il sequestro si presti a meccaniche esplorative, sebbene se ne denunzi un'esondazione nel perimetro della genesi normativa, cfr. DINACCI, *Sequestro di dispositivi informatici*, cit., 8 e ss. Sul punto, l'A. si domanda del perché l'attività di selezione postuma del materiale rilevante non possa essere fatta prima al momento del sequestro del dispositivo elettronico (*ivi*, 12).

[56] Corte giust. UE, C-548/21, cit., 92.

l'orientamento sessuale), i quali giustificano la protezione specifica di cui all'art. 10 della direttiva 2016/680[57]. In tali casi, afferma la Corte, l'ingerenza nei diritti della persona potrebbe qualificarsi anche come «particolarmente grave«[58].
Ma, ancora, rispetto a determinati soggetti, quali ad esempio il difensore, l'intrusione nel dispositivo potrebbe essere suscettibile di ledere ulteriori valori costituzionalmente tutelati, se si considera che oggigiorno la telematizzazione sta comportando la dematerializzazione degli scritti ed attività difensive. Si vuol dire che, qualora l'accesso al dispositivo informatico dovesse interessare un soggetto qualificato, quale il difensore, potrebbe (e forse dovrebbe) operarsi un'estensione delle garanzie di cui all'art. 103 c.p.p., norma dettata in tema di garanzie di libertà di tale soggetto processuale, la quale deve essere letta alla luce del "principio di effettività" della tutela, in tema di valutazione dei limiti e della legittimità della perquisizione e del sequestro presso (a questo punto) non solo lo studio del difensore, ma anche i suoi dispositivi informatici che utilizzi per la propria attività professionale[59].
Un intervento legislativo riformatore[60], dunque, deve farsi carico di prendere posizione rispetto alla necessità di tutela sia dell'ambito pubblicistico (e dunque a salvaguardia della effettività della funzione investigativa tanto nel versante

---

57 Trattasi di dati personali che rivelano l'origine razziale o etnica, le opinioni politiche e le convinzioni religiose o filosofiche. Si badi che la tutela offerta dalla direttiva si estende anche ai dati che rivelano indirettamente, a seguito di un processo intellettuale di deduzione o di controllo incrociato, informazioni di tale natura; Corte giust. UE, C-548/21, cit., 94; cfr., per analogia, Corte giust. UE, 5 giugno 2023, C-204/21, Commissione/Polonia, EU:C:2023:442, 344, in tema di indipendenza e privacy dei giudici.

58 Corte giust. UE, C-548/21, cit., 95.

59 Su tale argomento, la necessità che il tema della tutela del principio di legalità processuale debba essere valutata sul piano dell'effettività piuttosto che su quello del mero rispetto formale delle norme, cfr. BARGI, *Le garanzie di libertà del difensore tra formalismo interpretativo e effettività della legalità processuale*, in questa Riv., 2022, 2; l'A., di poi, sottolinea, a p. 6, come «l'estensione delle garanzie a tutti quei luoghi "presso" i quali i difensori – e gli altri soggetti ad essi equiparati – conservino la documentazione inerente all'attività difensiva, ribadisce, infatti, che le guarentigie di libertà della difesa a differenza della disciplina delineata dall'art. 253 c.p.p. - sono collegate direttamente anche alle persone».

60 Invero già "in cantiere", cfr. d.d.l. 806 del 19.7.2023, già approvato dal Senato ed attualmente all'esame della Camera, rubricato «Modifiche al codice di procedura penale in materia di sequestro di dispositivi e sistemi informatici, smartphone e memorie digitali» la cui finalità, come evidenzia PARODI, *Accesso ai dati presenti sul cellulare: quando, come e perché*, in www.rivistaildirittovivente.it, 11 ottobre 2024, appare quella di assicurare - in occasione del sequestro dei dispositivi sopra indicati e tenuto conto dei dati altamente sensibili in essi contenuti - garanzie al pari delle intercettazioni, prevedendo una selezione dei contenuti dei medesimi con le forme del contraddittorio tra le parti, funzionale a determinare cosa sia rilevante a fini processuali, anche in relazione alla conservazione dei dati nell'archivio digitale delle intercettazioni.

preventivo che repressivo) che della salvaguardia dei diritti fondamentali del privato cittadino coinvolto; e ciò sia che si tratti del diretto interessato dall'investigazione, sia che si tratti di un terzo estraneo alla stessa.
La pronunzia in discorso è, altresì, suscettibile di trovare applicazione alla problematica questione attinente all'utilizzo nel nostro ordinamento, durante la fase investigativa, degli IMSI *catchers*[61]. Come noto, tali strumenti sono apparecchi portatili, delle dimensioni d'una valigetta[62], che sfruttando alcune vulnerabilità delle reti di comunicazione, in particolare quelle che adoperano lo standard GSM, fingono di essere un ponte radio, in modo da indurre i cellulari nei dintorni ad agganciarsi e carpirne i codici identificativi[63]. Lo scopo di tale intrusione consiste nella possibilità successiva di farsi rilasciare tanto l'IMSI quanto l'IMEI, tappa preliminare a controlli ulteriori, tra cui l'inoculazione d'un trojan horse; oppure un'intercettazione destinata a colpire un telefono di cui ancora non si conosce il numero; o, ancora, ai fini di un "pedinamento elettronico"[64].
A ciò aggiungasi, come evidenziato dalla dottrina che tra le prime ha posto in luce la problematicità di tali strumenti di indagine[65], che la maggior parte dei modelli in commercio hanno anche funzioni aggiuntive (spesso vendute a parte, come softwares opzionali): possono infatti interrompere il servizio, impedendo la connessione alla rete[66]; registrare il contenuto delle comunicazioni inviate e ricevute[67]; fare chiamate o mandare messaggini per conto del telefono "in ostaggio"; cambiare il contenuto dei messaggi inviati[68]; esplorare e registrare quanto

[61] Per un approfondimento e spunti di riflessione, cfr. CAMON, *Il cacciatore di IMSI*, in *questa Riv.*, 2020, n. 1.
[62] BAJAK, *APNewsBreak: US suspects cellphone spying devices*, in www.apnesnew
[63] Ne riassume così la funzione CAMON, *Il cacciatore di IMSI*, cit., 2.
[64] OWSLEY, *TriggerFish, StingRays, and Fourth Amendment Fishing Expeditions*, 66 Hastings LJ, 2014, 193.
[65] CAMON, *Il cacciatore di IMSI*, cit., 3 e le relative citazioni bibliografiche anche qui riportate di seguito.
[66] ZETTER, *Turns out police stingray spy tools can indeed record calls*, in Wired, (www.wired.com/2015/10/stingray-government-spy-tools-can-record-calls-new-documents-confirm).
[67] LYE, *In Court: Uncovering Stingrays, A Troubling New Location Tracking Device*, in www.aclu.orgn; PAGLIERY, *FBI lets suspects go to protect «Stingray» secrets*, in money. cnn.com/2015/03/18/technology/security/police-stingray-phone-tracker/; PELL, SOGHOIAN, *A Lot More than a Pen Register, and Less than a Wiretap*, 16 Yale J.L. & Tech (2014), 143, nota 20, 146 e 148, nota 46; in re application of the United States of America for an order authorizing the use of a cellular telephone digital analyzer, 885 F. Supp. 197 (C.D. Cal. 1995).
[68] HEMMER, *Duty of candor in the digital age: the need for heightened judicial supervision of stingray searches*, 91 Chi.-Kent L. Rev., 2016, 296 s.

è archiviato nel dispositivo sotto controllo[69].
Non v'è dubbio, pertanto, della rilevante lesione alla sfera della *privacy* che tali strumentazioni sono suscettibili di operare, venendo in rilievo i valori salvaguardati agli artt. 8 CEDU e 7 CDFUE, trattandosi indiscutibilmente di una "tecnica di sorveglianza massiva"[70], non essendo tale modalità limitabile ad un determinato destinatario in quanto essa acquisisce i dati dei telefoni cellulari in maniera indiscriminata, bastando che essi rientrino nella sua sfera di attrazione territoriale.
Proprio per tali ragioni, passando al fronte della disciplina interna, lo schema processuale dettato dal vigente codice di rito in tema di libertà personale e del domicilio, nella scansione maggiormente garantita per come risultante dal combinato disposto delle previsioni costituzionali e codicistiche, sembra ben attagliarsi anche alla *subiecta materia*, risultando essi conformi ai dettami dei Giudici della Corte del Lussemburgo. Con la pronunzia in esame, in effetti, la Corte contempera le esigenze garantistiche del privato con quelle di salvaguardia delle investigazioni in maniera (sostanzialmente) analoga a come previsto nelle disposizioni del vigente codice di procedura dettata in tema di tutela delle libertà, ricalcando le sequenze procedimentali già previste all'art. 267 c.p.p. in tema di intercettazioni. L'unico elemento di novità, per vero non del tutto "nuovo" per la giurisprudenza nostrana in *subiecta materia*[71], è costituito dal vaglio di "proporzionalità" che deve guidare il Giudice nella ponderazione dei contrapposti interessi, criterio ad ogni modo non sconosciuto al nostro panorama normativo (in materia cautelare, in effetti, esso è già previsto all'art. 275 c.p.p.).
Quanto alla tutela anche del soggetto terzo rispetto alla vicenda investigativa,

---

[69] NORMAN, *Taking the sting out of the Stingray: the dangers of cell-site simulator use and the role of the Federal communications commission in protecting privacy & security*, 68 Fed. Comm. L.J., 2016, 141 ss.
[70] Così CAMON, *Il cacciatore di IMSI*, cit., 11.
[71] In effetti, DINACCI, *Sequestro di dispositivi informatici*, cit., 7 e ss. ed *ivi* in note 14 e 15, rileva come la Corte nomofilattica si sia adeguata al dovere di osservanza al principio di proporzionalità imposto dalla giurisprudenza della Piccola e della Grande Europa (Tra le tante v. Corte giust. UE, 3 dicembre 2019, C-482-17; Corte EDU, 23 gennaio 2025, Resnik v. Ucraina; Id., 19 dicembre 2024, Grande Oriente d'Italia c. Italia; Id., Grande camera, 16 luglio 2014, Alisic c. Bosnia ed Erzegovina; Id., Grande camera, 5 gennaio 2000, Beyeler c. Italia), assistendosi ad un'evoluzione giurisprudenziale che non ha inciso solo sui presupposti operativi del sequestro (Cfr. Cass., Sez. V, 18 maggio 2023 n. 1519, in *Foro.it*, 2024, 3, 132, laddove si è precisato che «il principio di proporzionalità è applicabile anche alle misure cautelari reali), ma ha anche declinato le modalità di azione rese più complesse dalla realtà informatrica su cui si è chiamati ad agire.

come già menzionato *supra*, la Corte si allinea alla giurisprudenza della Corte EDU, la quale si è espressa su questo specifico tema con pronunzia di condanna resa proprio nei confronti dell'Italia, ove si afferma la carenza della normativa italiana in punto di previsione, in favore di quei terzi estranei al procedimento ma destinatari di un provvedimento di intercettazione, di un'adeguata ed effettiva garanzia di controllo del provvedimento autorizzativo (quale la notifica anche successiva dello stesso), funzionale alla possibilità di impugnarlo retroattivamente[72]. Secondo la Corte di Strasburgo, allora, la normativa italiana comporta un inaccettabile rischio di abuso, con indubbia violazione dell'art. 8 della Convenzione. Lo Stato italiano dovrà prevedere la comunicazione alla persona che ha subito l'accesso dei "motivi su cui si basa l'autorizzazione di accesso a tali dati", dal momento in cui tale informazione non comprometta le esigenze del procedimento penale. Tale esigenza scaturisce dalla circostanza per cui per le persone non sospettate di reato e non coinvolte direttamente nel processo penale, la legge italiana non prevede la possibilità di chiedere in sede giudiziaria un controllo sulla "necessità" e sulla "legalità" del provvedimento con il quale è stata disposta l'intercettazione delle comunicazioni e, quindi, se del caso, prevedere una adeguata "riparazione"[73].
Il legislatore nazionale, dunque, anche sotto tale aspetto, è chiamato ad adeguarsi ai principi stabiliti dal Giudice europeo e, dunque, a prevedere un obbligo informativo riguardante l'accesso ai dati del dispositivo. Sicché, considerato che la vigente legislazione consente al P.M. ed alla P.G. (nei casi di urgenza) di procedere al sequestro per fini probatori di un bene mobile e, dunque, anche di un dispositivo elettronico, sarà necessario a questo punto che l'organo inquirente notifichi al proprietario del bene una comunicazione sulla volontà di procedere all'acquisizione dei dati in esso contenuti anche al fine di consentire al soggetto interessato di esperire i mezzi di impugnazione rispetto all'accesso ai dati. Sul punto, allora, se il rimedio del riesame *ex* artt. 257-324 c.p.p. è certamente idoneo allo scopo, esso dovrebbe avere ad oggetto la verifica di sussistenza delle condizioni indicate dalla Corte ai fini della compressione delle libertà fondamentali interessate. In altre parole, il giudizio deve estendersi al vaglio del provvedimento autorizzativo giurisdizionale, col

[72]Corte EDU, 23 maggio 2024, Contrada c. Italia, 92-97; per un commento, GIORDANO, *Considerazioni sulla sentenza della Cedu Contrada c. Italia n. 4: per un'interpretazione convenzionalmente orientata delle norme di codice di rito*, in *Sis. pen.*, 26/06/2024, reperibile al link https://www.sistemapenale.it/it/scheda/giordano-considerazioni-sulla-sentenza-della-cedu-contrada-c-italia-n-4
[73] Così FILIPPI, *op. cit.*

quale è stato autorizzato l'accesso ai dati nel dispositivo elettronico, ed in particolare l'uso del giudizio ponderativo fondato sul criterio di proporzionalità. Sotto altro profilo, occorrerebbe domandarsi altresì dei possibili effetti diretti che tale pronunzia potrebbe esplicare nei confronti dei processi in corso[74]. Invero, a seconda che si ritenga che la direttiva 680/2016 UE - per come interpretata dalla presente decisione - esplichi o meno effetti diretti nell'ordinamento nazionale, potrebbero conseguire effetti rispetto alla valutazione del dato probatorio acquisito in difformità delle statuizioni della Corte di giustizia. In altre parole, il dato probatorio così acquisito potrebbe essere ritenuto inutilizzabile o meno in ragione della violazione del diritto fondamentale alla privacy sancito da tale fonte europea, oltre che dall'art. 8 CEDU[75].

[74] Sulla cogenza delle pronunzie della Corte di giustizia UE, cfr. DINACCI, *Interpretazione "europeisticamente" orientata: tra fonti normative e resistenze giurisprudenziali*, in *Cass. pen.*, 2016, 3055; ed ancora, ID., *I modi acquisitivi della messaggistica chat o e-mail*, cit., 9-10.

[75] Si esprime in termini di inutilizzabilità, ma anche di violazione del parametro dell'equo processo, DINACCI, *Sequestro di dispositivi informatici*, cit., 39.