QUESITI

ELENA ANDOLINA

La raccolta dei dati relativi alla localizzazione del cellulare ed al traffico telefonico tra inerzia legislativa e supplenza giurisprudenziale

Mentre, in ambito europeo, in attesa della conclusione dei negoziati relativi al Regolamento e-*Privacy* destinato ad abrogare la direttiva 2002/58/CE, la Corte di giustizia UE *post Tele2Sverige* è impegnata a precisare i limiti entro i quali le autorità nazionali possono acquisire i *traffic data* a fini di giustizia penale, sul piano interno faticano ad imporsi i principi di legalità e di proporzione. Segnatamente, in materia di tracciamento dell'utenza telefonica mobile e di acquisizione dei tabulati telefonici, la giurisprudenza di legittimità, nell'esercizio di improprie funzioni di supplenza, appare incline ad assecondare ora prassi investigative illegittime elusive della stretta legalità processuale, ora interpretazioni distorte, ed antiformalistiche, del canone di proporzione.

The collection of data relating to the location of the mobile phone and telephone traffic between legislative inertia and jurisprudential substitution.

While, in the European context, pending the conclusion of the negotiations relating to the e-Privacy Regulation intended to repeal Directive 2002/58 / EC, the post-Tele2Sverige Court of Justice UE is committed to specifying the limits within which national authorities can acquire traffic data for criminal justice purposes, on the internal level the principles of legality and proportion struggle to impose themselves. In particular, in the matter of tracking mobile telephone users and the acquisition of telephone records, the jurisprudence of legitimacy, in the exercise of improper substitute functions, appears inclined to indulge now illegal investigative practices elusive of the strict procedural legality, now distorted interpretations, and anti-formalistic, of the canon of proportion.

SOMMARIO: – 1. Tecnologie di controllo telefonico non ancora normate: il tracciamento del dispositivo di telefonìa mobile. – 2. Inquadramento dogmatico del tracciamento e futuribile assetto normativo. 3. (Segue). L'attuale deprecabile vuoto di garanzie. – 4. La *data retention* nella giurisprudenza della Corte di giustizia UE. – 5. Il mancato adeguamento dello *jus conditum* ai *dicta* della Corte di Lussemburgo. – 6. L'esorbitante innalzamento dei tempi di conservazione dei dati di traffico. – 7. La ricostruzione "deformante"del *proportionality check* nella giurisprudenza nazionale. – 8. (Segue). Il diritto vivente eurounitario.

1. *Tecnologie di controllo telefonico non ancora normate: il tracciamento del dispositivo di telefonìa mobile*. Significative compressioni dei diritti fondamentali della persona possono conseguire al ricorso, a fini investigativi, a quelle metodologie di sorveglianza segreta preposte alla raccolta automatizzata dei dati personali meta-individuali[1], trattati in una rete di comunicazione elettronica ed integranti le "tracce" dell'interazione dell'individuo nella società

[1] Sulle potenzialità della raccolta ed aggregazione dell'insieme di tali dati personali ai fini della prevenzione e persecuzione dei reati nell'ordinamento processuale del XXI secolo, v. COSTANZI, *Big data e garantismo digitale. Le nuove frontiere della giustizia penale nel XXI secolo,* in *Leg. pen.,* 2019.

iper-tecnologica dell'informazione[2].
In questo contesto, ci soffermeremo sulle tecniche di controllo telefonico che consentono ora l'apprensione dinamica, in tempo reale, dei dati relativi alla posizione geografica dell'utenza telefonica mobile; ora l'acquisizione *a posteriori* dei dati esterni identificativi delle comunicazioni telefoniche (numeri dell'utente chiamante e chiamato, luogo, data, ora, durata della comunicazione), archiviati dall'ente gestore del servizio di telefonìa nei cd. tabulati telefonici (o telematici).
Sotto il primo profilo viene impiegato il termine "tracciamento", o localizzazione dell'utenza telefonica mobile (cd. "*contact tracing*"), con riferimento alla specifica modalità di sorveglianza fisica tecnologicamente assistita, finalizzata al monitoraggio dinamico degli spostamenti sul territorio del telefono cellulare (*smartphone* o *tablet* dotato di connessione), e riconducibile al *genus* delle operazioni investigative di geolocalizzazione[3] (di cose o persone).
Va stigmatizzato, sin da subito, come, a dispetto dell'estrema rilevanza ai fini della ricostruzione delle dinamiche del reato[4], nonché della potenziale lesività, la localizzazione tecnologica continui ad essere inopinatamente trascurata dal legislatore.
Per vero, si è persa, nel quadro dei recenti interventi riformistici in materia di intercettazioni - prima il d.lgs. 29 dicembre 2017, n. 216, poi il d.l. 30 dicembre 2019, n. 161, conv. in l. 28 febbraio 2020, n. 7 -, l'ennesima occasione non solo per un adeguamento generale dell'attività investigativa ai nuovi strumenti di indagine ad elevato contenuto tecnologico[5], ma, anche, per una revi-

[2] Tecnologie che, pur senza cognizione di dati fonici o flussi comunicativi, incidono (anche) sulla segretezza delle comunicazioni, così da essere classificate, in dottrina, come «forme di non-intercettazione» (cfr. APRILE, SPIEZIA, *Le intercettazioni telefoniche ed ambientali. Innovazioni tecnologiche e nuove questioni giuridiche*, 2004, Milano, 125 ss.).

[3] Su tale neologismo, introdotto a partire dalla seconda metà del XX secolo in corrispondenza con lo sviluppo delle tecnologie dell'informazione, cfr. COSTANZO, *Note preliminari sullo statuto giuridico della geolocalizzazione (a margine di recenti sviluppi giurisprudenziali e legislativi)*, in *Dir. inform.*, 2014, 3, 331.

[4] Di estrema attualità sono, poi, i diversi, ed ulteriori, àmbiti applicativi, in cui sono utilizzabili le preziose informazioni offerte dalla mappatura degli spostamenti sul territorio – non ultimo l'àmbito sanitario ai fini di contenimento del contagio del Sars-Cov (v., al riguardo, l'intervento di Antonello Soro, in Agenda Digitale, 29 marzo2020) - o dal controllo a distanza della posizione del lavoratore, sulla base dei rilievi del GPS installato all'interno di veicoli aziendali in dotazione del primo.

[5] Si fa riferimento sia allo strumento, altamente intrusivo, preposto alla raccolta di dati di natura visiva – le video riprese –, sia a tutte quelle prassi investigative, oltremodo lassiste, collaudate da tempo, come l'"agente segreto attrezzato per il suono" e l'acquisizione urgente dei dati segnalati sul *display* di un apparecchio di telefonìa mobile entrato nella disponibilità delle forze di polizia. Relativamente più recente è, poi, lo strumento del "*code catcher*", impiegato dalla polizia giudiziaria per catturare i codici identifi-

sione della normativa relativa alla captazione dei dati esterni delle comunicazioni telefoniche in aderenza agli *standard* europei[6].
Un preoccupante vuoto normativo che, nello specifico àmbito che ci occupa, investe la geolocalizzazione tanto se eseguita, tramite le celle della rete telefonica, ponendo sotto controllo il dispositivo di telefonìa mobile in uso al soggetto monitorato (*Global System Mobiles-GSM*), quanto se attuata mediante un sistema di rilevamento satellitare (*Global Positioning System* - GPS) installato e/o occultato su un oggetto nella disponibilità di una persona (di regola, un'automobile) o direttamente sullo stesso soggetto monitorato.
Al fine di decifrare la natura giuridica, ancora in ombra e non sufficientemente esplorata, dell'operazione di tracciamento, fugando, al contempo, eventuali confusioni sul piano concettuale, v'è da segnalare come l'acquisizione dinamica, in tempo reale, dei dati relativi all'ubicazione del telefono cellulare (ed indirettamente del suo detentore) possa avvenire sia nella forma del "tracciamento delle comunicazioni"- comunemente noto anche come "tracciato AXE" - [7] all'atto dell'effettuazione della conversazione telefonica e in occasione dell'ascolto della fonìa; sia nella forma del tracciamento dell'utenza telefonica mobile in modo indipendente e autonomo rispetto all'operazione intercettiva.
Non può obliterarsi la differenza logica e materiale intercorrente tra le due tecniche di tracciamento. Nell'ipotesi di tracciamento delle comunicazioni

---

cativi – *IMSI* della *Sim Card* e *IMEI* - dei cellulari che si trovano in una certa area (sul punto, CAMON, *Il cacciatore di Imsi,* in *questa Rivista,* 2020, 1). Sull'impatto dell'evoluzione tecnologica sul processo penale - ampiamente messo in luce in dottrina - da ultimo: CONTI, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo*, in *Dir. pen. proc.*, 2018, 9, 1210 ss.; FELICIONI, *Le fattispecie "atipiche" e l'impiego processuale*, in *L'intercettazione di comunicazioni*, a cura di Bene, Bari, 2018, 303 ss.; FERRUA, Presentazione, in *La prova scientifica nel processo penale*, a cura di Carlizzi, Tuzet, Torino, 2018, 4 ss.; LORUSSO, Digital evidence, cybercrime *e giustizia penale*, in *Proc. pen. giust.*, 2019, 4, 821 ss.; NOCERINO, *Il captatore informatico: un giano bifronte. Prassi operative vs. risvolti giuridici*, in *Cass. pen.,* 2020, 2, 824; SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018, 11 ss.

[6] Su cui, *infra,* par. 4 ss.

[7] Così si definisce quella tecnica investigativa originata dall'evoluzione della procedura di "blocco" della chiamata, cioè l'arresto degli organi di commutazione del circuito su tutta la rete, attraverso cui «si poteva materialmente seguire il tracciato della comunicazione all'interno della rete stessa e così individuare la linea del soggetto chiamante»: cfr. DE LEO, *Controllo delle comunicazioni e riservatezza (a proposito di tabulati, tracciamenti, intercettazioni, conservazione dei dati e dintorni)*, in *Cass. pen.,* 2002, 2208. Sul punto, v., pure, APRILE, SPIEZIA, *Le intercettazioni telefoniche ed ambientali. Innovazioni tecnologiche e nuove questioni giuridiche*, cit., 143, e FILIPPI, *Il rilevamento del "tracciato* axe": *una nuova denominazione per una vecchia tecnica d'indagine*, in *Giur. it.,* 1999, 1689.

telefoniche e telematiche - oggetto, tra l'altro, di un esplicito riconoscimento normativo nel limitato contesto delle investigazioni preventive (all'art. 226, co. 4, disp. coord. c.p.p.) - le autorità inquirenti prendono cognizione, contemporaneamente ai contenuti comunicativi, e in modo automatico, (anche) dei dati esterni associati alla comunicazione telefonica in corso (*id est*, dei dati di traffico), tra i quali rientrano quelli identificativi della posizione geografica del telefono cellulare sul territorio.
Di talchè, attesa la simultaneità tra operazione intercettiva e raccolta dei dati esteriori dell'atto comunicativo documentati dal tracciato *axe*, l'attività di tracciamento (o rilevamento del tracciato *axe*) non può che sottostare alle stesse garanzie previste per le intercettazioni foniche di flussi informatici di cui all'art. 266-*bis* c.p.p. e, come tale, essere autorizzata dal giudice con lo stesso provvedimento autorizzativo dell'operazione intercettiva[8]. Ben diversa dalla precedente è l'ipotesi in cui gli organi investigativi, in possesso del numero seriale identificativo dell'apparecchio telefonico mobile - il cd. codice *Imei* (*International Mobile Equipment Identity*) - intendano solo tracciarne, in tempo reale, gli spostamenti del terminale o, all'inverso, monitorare le utenze presenti in una determinata zona al fine di individuare i codici identificativi di un dato cellulare. In tale evenienza, il controllo dinamico dell'utenza telefonica, in quanto espletabile, anche, a prescindere da un atto comunicativo, potrebbe non essere agganciato a una comunicazione in corso; e i dati relativi all'ubicazione del dispositivo non inerire al traffico telefonico.

2. *Inquadramento dogmatico del tracciamento e futuribile assetto normativo.*
Attesa la perdurante indifferenza del legislatore, occorre interrogarsi sul regime giuridico di tale specifica forma di tracciamento.
Seppur non specificamente normata, l'operazione di monitoraggio dinamico degli spostamenti del cellulare trova, comunque, un sicuro fondamento nel Codice in materia di protezione dei dati personali (cd. Codice della *privacy*), il d.lgs. 30 giugno 2003, n. 196, recentemente modificato dal d.lgs. 10 agosto

[8] Per vero, attesa la trasmissione dei dati telefonici alle centrali di ascolto presso la procura «sulla base di flussi di dati numerici (*bit*) in movimento nella rete», l'attività di acquisizione del tracciato *axe* «non è che il risultato di una forma di intercettazione informatica» riconducibile all'art. 266-*bis* c.p.p.: cfr. ZACCHÈ, *Acquisizione di dati esterni ai colloqui telefonici*, in *Dir. pen. proc.*, 1999, 340. Conf. DE LEO, *Controllo delle comunicazioni e riservatezza (a proposito di tabulati, tracciamenti, intercettazioni, conservazione dei dati e dintorni)*, cit., 2210, e VIALI, *L'acquisizione dei dati esteriori di conversazioni o comunicazioni: tra nuove tecnologie e sbandamenti giurisprudenziali,* in *Cass. pen.*, 1999, 2583. , in questa rivista, 1999, p. 2576, n. 1284

2018, n. 101, in adeguamento al regolamento UE 2016/679 (GDPR)[9]. Venendo in rilievo il combinato disposto dell'art. 121, co. 1 *bis*, lett. *i)*[10] - come interpolato dal d.lgs. n. 101 del 2018 - e dell'art. 126, co. 1, Codice della *privacy*, là dove consente il trattamento dei «dati relativi all'ubicazione diversi dai dati relativi al traffico, riferiti agli utenti o ai contraenti di reti pubbliche di comunicazione o di servizi di comunicazione elettronica accessibili al pubblico»[11].

A rendere più problematico il suo inquadramento dogmatico sembra, poi, contribuire la natura eterogenea dei dati acquisibili mediante l'attività di localizzazione dinamica del dispositivo di telefonìa mobile. Non potendosi prognosticare, nel momento in cui l'operatore pone sotto controllo l'apparecchio, se interverranno o meno eventuali comunicazioni telefoniche (in entrata o in uscita)[12], è, infatti, possibile che insieme a dati di ubicazione non connessi al traffico telefonico vengano, altresì, in rilievo dati di traffico.

Proprio nella peculiare natura di tali dati personali non comunicativi - oggetto di captazione - suscettibili di essere, al contempo, dati di traffico telefonico, risiede il tratto caratterizzante questa modalità di geolocalizzazione dinamica e la chiave di lettura per decifrarne il futuribile, e non più procrastinabile, assetto normativo. Per vero, a differenza del "pedinamento elettronico" tramite sistema GPS, il tracciamento dell'utenza telefonica mobile si specifica per l'attitudine ad incidere pure sulla segretezza delle comunicazioni; potendo svolgersi in coincidenza con l'effettuazione (o ricezione) di una telefonata. In

---

[9] Il regolamento UE 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE, ha trovato applicazione diretta in tutti i Paesi UE a partire dal 25 maggio 2018. Esso compone il nuovo "pacchetto europeo sulla protezione dei dati personali" del 27 aprile 2016, insieme alla Direttiva UE 2016/680 (entrata in vigore il 5 maggio 2016), relativa alla protezione delle persone fisiche, con riguardo al trattamento dei dati da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, che abroga la decisione quadro 2008/977/GAI.

[10] Ai sensi dell'art. 121 (Servizi interessati e definizioni), co. 1-*bis*, lett. *i)*, Codice della *privacy* - in cui è confluito il contenuto dell'abrogato art. 4 (Definizioni), co. 2, lett. *l)* – per "dat[o] relativ[o] all'ubicazione" s'intende «ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica, che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico».

[11] A queste conclusioni è, già, pervenuto sulla base del previgente art. 4, co. 2, lett. *l)* e dell'art. 126 Codice della *privacy,* CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni,* in *Riv. it. dir. proc. pen.*, 2005, 2, 631-632.

[12] Cfr. DI PAOLO, *Tecnologie del controllo e prova penale: l'esperienza statunitense e spunti per la comparazione*, Padova, 2008, 260, nota 237.

ogni caso, al di là della possibile incidenza sull'art. 15 Cost., non può più revocarsi in dubbio che il controllo dinamico degli spostamenti di una persona sul territorio (sia tramite celle telefoniche che tramite *tracker* GPS), sebbene si attui in pubblico e, dunque, riguardi persone esposte all'osservazione generale altrui, interferisce sul diritto alla vita privata della persona, tutelato dagli articoli 8 CEDU, nonchè 7 e 8 CDFUE, sia pure con minore intensità rispetto ai più incisivi metodi di sorveglianza visiva o acustica[13].

Come, infatti, è stato ben evidenziato dai giudici di Strasburgo, il bene «vita privata» di per sé inafferrabile e «non suscettibile di definizione esaustiva» «[...]protegge, *inter alia*, [...] il diritto di stabilire e sviluppare relazioni con altri esseri umani e con il mondo esterno»[14]; ed è, dunque, tale da coprire «una zona di interazione tra l'individuo e gli altri», anche se si svolge in un contesto pubblico, *id est* al di fuori del domicilio e dei luoghi di privata dimora[15].

Per vero, a partire dalla seconda metà del XX secolo, alla crescente esposizione pubblica della persona correlata alle nuove tecnologie dell'informazione e, dunque, al passaggio da situazioni di intimità a situazioni di *extimité*[16] è corrisposta una dilatazione della nozione di "vita privata", concetto di per sè fluido e in costante evoluzione[17]. Si è così transitati, grazie, segnatamente, all'interpretazione evolutiva della Corte EDU, dalla dimensione negativa e statica di vita privata-intimità, come diritto ad essere lasciato solo ("*right to be let alone*")[18], basato su una ristretta logica dominicale, ad una più

---

[13] Corte EDU, sent. 2 settembre 2010, Uzun c. Allemagne; conf. Corte EDU, sent. 8 febbraio 2018, Ben Faiza c. Francia.

[14] Corte EDU, sent. 2 settembre 2010, cit., § 40.

[15] Cfr., con riferimento a sistemi a circuito chiuso di videosorveglianza e controllo delle vie cittadine, Corte EDU, sent. 28 gennaio 2003, Peck c. Regno Unito, § 57 e, con riguardo alle registrazioni di conversazioni tenute dal detenuto nel parlatorio all'interno delle carceri, in occasione dei colloqui con i prossimi congiunti, Corte EDU, sent. 20 dicembre 2005, Wisse c. Francia.

[16] Cfr. RODOTÀ, *Prefazione*, in *Libera circolazione e protezione dei dati personali*, a cura di Panetta, Milano, 2006, t. I, VIII-IX.

[17] In virtù della stretta relazione esistente tra progresso tecnologico e mutamenti del concetto di *privacy* (cfr. RODOTÀ, *La privacy tra individuo e collettività*, in *Pol. dir.,* 1974, 551), il diritto alla *privacy* viene assunto come «paradigma [dei] diritti "liquidi", ossia anamorfici o metamorfici in quanto privi di connotati durevoli e stabili» (cfr. CISTERNA, *Cedu e diritto alla* privacy, in *Principi europei del processo penale*, a cura di Gaito, Roma, 2016, 194).

[18] Corrispondente al contenuto originario della *privacy*, il "diritto ad essere lasciato solo" è stato teorizzato alla fine del XIX secolo da due avvocati di Boston - WARREN e BRANDEIS, *The Right to Privacy*, IV *Harvard Law Review*, 193(1890) - trovando, poi, riconoscimento nella giurisprudenza americana (sul punto, RIGAUX, *L'élaboration di un "right to privacy" par la jurisprudence amèricaine,* in *Rev. intern. dr. comp.,* 1980, 701 ss.).

ampia e poliedrica nozione di *privacy* giuridicamente rilevante; nella cui sfera, accanto ai tradizionali profili di tutela connessi alla riservatezza (intimità, domicilio, segretezza), sono ricompresi nuovi e ulteriori profili attinenti all'identità esterna della persona (come il diritto alla protezione dei dati personali ed all'autodeterminazione informativa).

Proprio alla dimensione dinamica e relazionale di vita privata-libertà appare riconducibile il diritto a restare anonimi nell'esplicazione delle proprie libertà personali, ovvero ad interagire con il mondo esterno in modo anonimo[19]. Su questa fondamentale proiezione della libertà di autodeterminazione dell'individuo, sotto il profilo del diritto a controllare il trattamento dei propri dati personali (*id est,* le tracce delle proprie relazioni sociali)[20], poggia la ragionevole aspettativa individuale a essere "irrintracciabili" e a non venire localizzati[21], mediante strumenti di sorveglianza tecnologica, anche là dove si agisca in un luogo pubblico o aperto al pubblico.

Infatti, se, da un canto, la scelta individuale di utilizzare una delle nuove, e sofisticate, generazioni di cellulari - come pure quella di esporsi in spazi pubblici - implica la rinuncia ad una parte della propria riservatezza, limitatamente ad alcune informazioni personali[22]. Dall'altro canto, non può disconoscersi l'interesse dell'individuo a non essere del tutto controllabile e, nel caso specifico, la legittima aspettativa di riservatezza, in capo all'utente di apparecchi telefonici mobili, ad essere tutelato nell'uso di siffatti dispositivi tecnologici di

---

[19] Il cd. diritto all'anonimato ("*the right to anonymity*") è stato teorizzato dalla dottrina statunitense come una delle quattro dimensioni della privacy: *solitude, intimacy, anonimity, repose* (SLOBOGIN, *Public Privacy camera surveillance of public places and the right to anonymity*, in 72 *Mississipi Law Journal*, 213(2002), e WESTIN, *Privacy and freedom*, London, 1967, 31). Pur non essendo sancito espressamente dalla nostra Carta costituzionale, trova un esplicito riconoscimento nell'art. 10 (Protezione dell'anonimato) della Dichiarazione dei Diritti in Internet - redatta il 28 luglio 2015 dalla Commissione di studio presieduta da Stefano Rodotà - integrante, però, solo un documento politico, privo di valore giuridico.

[20] Sulla più ampia garanzia di *habeas data* elaborata in America latina dalla seconda metà del secolo XX e comprensiva del diritto alla protezione dei dati personali, della libertà di informazione e della libertà informatica, cfr. PÉREZ, ROBLEDO, *El procedimento de habeas data,* Madrid, 2017, 221 ss.; ROZO ACUÑA, Habeas data *costituzionale: nuova garanzia giurisdizionale del diritto pubblico latino-americano Dir. pubbl. comp. eur.*, 2002, 1922.

[21] Il diritto a non essere rintracciati, o localizzati, riconducibile all'art. 16 Cost. quale «componente della libertà di circolazione» (cfr., CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni,* cit., 632-633), trova, pertanto, pure un fondamento infra/para-costituzionale negli artt. 8 CEDU e 7-8 CDFUE.

[22] Come osservato - con specifico riguardo alla geolocalizzazione mediante rilevamento satellitare - dalla Corte EDU «un individuo che cammina per strada sarà inevitabilmente visibile ad altri componenti della società che sono presenti» (sent. 2 settembre 2010, cit., § 41).

comunicazione in rete[23] da un monitoraggio occulto, capillare e prolungato nel tempo che prescinda da qualsivoglia limite e garanzia adeguata a prevenire possibili abusi.
Di talchè, preso atto che la rilevazione a distanza degli spostamenti sul territorio, tramite il cellulare nella disponibilità del soggetto monitorato (o *tracker* GPS), implica il trattamento sistematico dei dati di ubicazione – risultando, perciò, maggiormente invasiva della sfera privata rispetto al pedinamento eseguito personalmente con osservazione visiva degli spostamenti[24] –, la stessa per essere tollerabile dovrà conformarsi alle specifiche condizioni di legittimità previste dall'art. 8, par. 2 CEDU (legalità, necessità e scopo).
Non solo. Potendo prospettarsi, con riferimento all'acquisizione dinamica dei dati relativi all'ubicazione del dispositivo di telefonìa mobile, oltre alla compressione della vita privata e della libertà di circolazione tutelata dall'art. 16 Cost., anche l'intrusione sulla segretezza delle comunicazioni, deve riconoscersi il vincolo - d'ordine costituzionale, nonché infra e para-costituzionale - del legislatore ad uniformarne il relativo regime a quello dell'acquisizione *ex post* dei dati di trafficoo[25], magari in occasione, e nel contesto, dell'auspicabile adeguamento della normativa in materia di *data retention* ai *dicta* della Corte di giustizia UE. Subordinandosi, pertanto, il ricorso alla tecnica di sorveglianza in esame allo stesso livello minimo di garanzie; così da superare l'attuale incoerenza del sistema che, rispetto alla stessa tipologia di dati, mentre ne regolamenta l'apprensione *a posteriori*, resta, invece, del tutto indifferente là dove si debbano acquisire in tempo reale, malgrado l'elevata probabilità che si tratti di dati di traffico.

3. *(Segue). L'attuale deprecabile vuoto di garanzie.*

[23] Una legittima aspettativa di riservatezza che, attesa l'assimilabilità del cellulare ai *computer*, appare, altresì, riconducibile al "diritto fondamentale alla garanzia dell'integrità e della riservatezza dei sistemi informatici", enucleato dalla Corte tedesca ed inteso come espressione del più generale diritto alla dignità dell'individuo-utente (sentenza del *Bundesverfassungsgericht* del 27 febbraio 2008 sulla c.d. *online durchsuchung*, in *Riv. trim. dir. pen. econ.*, 3, 2009, 679 e ss., con nota di Flor).

[24] Cfr. FANUELE, *Il rilevamento satellitare tramite Gps: una prassi da ancorare ai principi stabiliti dalla Cedu*, in *Dir. pen. proc.* 2019, 12, 1705, la quale sottolinea come si tratti di «una forma di pedinamento assai "più evoluta" per le cognizioni scientifiche presupposte e "più sofisticata" per la peculiare tecnica applicata» di quello tradizionale; consentendo un monitoraggio preciso e continuo degli spostamenti di un individuo, anche là dove gli stessi non siano altrimenti visibili ed il pedinamento tradizionale sarebbe impraticabile.

[25] Un auspicabile assetto normativo unitario viene prospettato, pure, da BRUNO, *La "localizzazione"elettronica tra indagine e prova*, in *Giust. pen.*, III, 12, 2011, 701 ss., e CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni*, cit., 631-632.

Una volta messo in luce il carattere affatto "innocuo" del tracciamento del cellulare, stante l'articolato quadro di diritti fondamentali suscettibili di lesione, non può che sconfessarsi l'indirizzo svalutativo su cui è da tempo consolidata la giurisprudenza di legittimità; alla quale, in assenza di una specifica regolamentazione, si è, di fatto, lasciato il compito di determinare lo statuto giuridico dell'attività di geolocalizzazione dinamica degli spostamenti sul territorio.

Secondo il diritto vivente, la procedura di tracciamento dell'apparecchio cellulare, tramite "*Global System Mobiles-GSM*"- come, del resto, pure la localizzazione tramite GPS[26] - costituirebbe una modalità tecnologicamente caratterizzata di pedinamento, rientrante tra gli atti urgenti e innominati demandati, ai sensi degli artt. 55 e 348 c.p.p., alla libera disponibilità degli organi della polizia giudiziaria. Escludendosi, pertanto, sulla base dell'erroneo postulato della non lesività dei diritti fondamentali, la possibilità di assimilare tali tecniche non solo all'attività di intercettazione[27], ma pure a quella finalizzata all'acquisizione di tabulati telefonici[28] e, dunque, la soggezione sia alla preventiva autorizzazione del giudice, sia al decreto motivato del pubblico ministero.

Si tratta, all'evidenza, di una prassi investigativa illegittima, oltrechè anacronistica[29], perché elusiva della regola di esclusione probatoria desumibile dal

---

[26]Sulla geolocalizzazione tramite GPS si rinvia a BENE, *Il pedinamento elettronico: truismi e problemi spinosi*, in *Le indagini atipiche*, a cura di Scalfati, Torino, 2014, 347 ss.

[27]Cass., Sez. I, 13 maggio 2008, Stefanini, in *Cass. pen.*, 2009, 2076; conf. Id., Sez. III, 27 febbraio 2015, Diano, in *Mass. Uff.,* n. 326999.

[28]Cass., Sez. IV, 12 giugno 2018, Chirico e a., n. 41385, secondo cui il monitoraggio dell'utenza presente in una determinata area, finalizzato all'individuazione dell'identità del singolo apparecchio telefonico (codice IMEI) da sottoporre a intercettazione telefonica, «non operando alcuna intrusione nelle conversazioni in transito sull'apparecchio monitorato e non essendo neppure finalizzato ad acquisire elementi sugli eventuali contatti telefonici che tale apparecchio intrattiene in un determinato arco temporale (talchè neppure potrebbe parlarsi, a ben vedere, di attività assimilabile all'acquisizione di tabulati telefonici, acquisibili sulla base di autorizzazione del Pubblico ministero: cfr. Cass, Sez. IV, 25 marzo 2009, La Rosa e altro, in *Mass. Uff.,* n. 244384), non necessita di un decreto autorizzativo, in quanto non lesivo di alcun principio costituzionale e sovranazionale».

[29]Ciò alla luce di quanto statuito non solo dalla Corte EDU, ma pure da altri consessi giurisdizionali: si pensi alla Corte Suprema americana che - dopo aver ravvisato nel pedinamento satellitare mediante GPS un atto contrario alla Costituzione federale (caso U.S v. *Jones*, 23 gennaio 2012) – ha recentemente ritenuto necessario il mandato del giudice al fine di acquisire i dati che consentono la geolocalizzazione attraverso le celle telefoniche, pena la violazione del IV Emendamento della Costituzione federale, e salve le ipotesi di eccezionale urgenza e gravità (caso *Carpenter v. United States* del 28 giugno 2018: sul punto, LIPTAK, *In Ruling on Cellphone Location Data, Supreme Court Makes Statement on Digital Privacy*, in New York Times, 22 giugno 2018).

principio di stretta legalità processuale posto dalla norma generale di garanzia di cui all'art. 111 co. 1 Cost., come integrato dalle specifiche disposizioni costituzionali, nonché dalle fonti di rango infra/para-costituzionale, che ammettono limitazioni ai diritti fondamentali nei soli casi e modi stabiliti dalla legge[30].

Per vero, non possono "camuffarsi" come atipiche modalità investigative, non normate, che recano *vulnus* a sfere di libertà costituzionalmente rilevanti e, come tali, riconducibili all'area delle prove incostituzionali[31].

Sicchè, fino a quando la tecnica di geolocalizzazione non sarà espressamente regolata dal legislatore in conformità agli *standard* di garanzia convenzionali e costituzionali - sulla falsariga di quanto già avvenuto in altri paesi[32] - i relativi dati probatori devono considerarsi inammissibili e processualmente inutilizzabili *ex* art. 191 c.p.p. Esito, questo, inconfutabile, in forza dell'art. 160-*bis* Codice della *privacy*[33], richiamato dall'art. 2-*decies* (Inutilizzabilità dei dati), che sottopone alla disciplina delle «*pertinenti disposizioni processuali [...] la validità, l'efficacia e l'utilizzabilità nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a disposizioni di legge o di Regolamento*».

4. *La* data retention *nella giurisprudenza della Corte di giustizia UE.*

Neppure l'archiviazione ed acquisizione dei dati esteriori delle comunicazioni telefoniche e telematiche si sottrae a sicure censure di legittimità, stante il perdurante contrasto dell'odierno assetto normativo di cui all'art. 132 Codice della *privacy* con gli *standard* di garanzia enucleati, alla stregua del sistema di

---

[30] Sul principio di legalità sul versante del procedere, quale inderogabile limite di ammissibilità della prova incidente su beni costituzionalmente rilevanti, sia consentito rinviare al nostro, *L'ammissibilità degli strumenti di captazione dei dati personali tra standards di tutela della privacy e onde eversive*, in *questa Rivista*, 2015, 3, 923.

[31] La categoria dogmatica della "prova incostituzionale"è stata enucleata dalla Corte costituzionale con riguardo a tutte quelle prove «ottenute attraverso modalità, metodi e comportamenti realizzati «in dispregio dei fondamentali diritti del cittadino» garantiti dalla Costituzione (Corte cost., sent. 6 aprile 1973, n. 34, in *Giur. cost.*, 1973, 338). Sul punto, CONTI, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo*, in *Dir. pen. proc.*, 2018, 9, 1211 e EAD., *Accertamento del fatto e inutilizzabilità nel processo penale*, Padova, 2007, 151 ss.

[32] Come la Francia che, con la legge del 28 marzo 2014 n. 372 (consultabile in *www.legifrance.gouv.fr.*; per un commento, cfr. CENCETTI, Je ne regrette rien: *Libertà della prova e legislazione francese in materia di sorveglianza tramite GPS*, in *www.diritti-comparati.it)*, si è uniformata alla giurisprudenza della Corte EDU*,* nonché a quelle della propria Corte di Cassazione (sentenza del 22 ottobre 2013).

[33] In quest'articolo è stato trasfuso il contenuto del vecchio art. 11, comma 2, Codice della *privacy*, abrogato dal D.lgs. 2018 n. 101.

tutela multilivello dei diritti fondamentali di cui agli artt. 7, 8 e 52, par. 1, CDFUE, dalla Corte di giustizia UE nella storica sentenza *Digital Rights Ireland e Seitlinger* [34].

Più nel dettaglio, i Giudici di Lussemburgo, dopo aver messo in luce che i metadati generati dalle comunicazioni, in quanto «dati personali, per così dire qualificati» [35], «presi nel loro complesso [consentono di] trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono conservati» [36], creando una mappatura di una parte importante dei comportamenti di una persona, «se non addirittura un ritratto completo [...] della sua identità privata» [37], dichiaravano invalida la direttiva 2006/24/CE (cd. direttiva Frattini). Quest'ultima, imponendo una conservazione generalizzata, ed incondizionata, dei dati di traffico telefonico e telematico, «allo scopo di garantirne la disponibilità a fini di indagine, accertamento e perseguimento di reati gravi», s'ingeriva in modo «particolarmente grave» nei diritti fondamentali garantiti dagli articoli 7 e 8 CDFUE, eccedendo i limiti imposti dal principio di proporzionalità.

Per vero, come precisato dalla Corte di giustizia UE, sebbene la *data rention* sia di per sè idonea in astratto a realizzare l'obiettivo legittimo prefissato, attesa l'elevata potenzialità euristica ed utilità dei *traffic data* per le indagini penali; cionondimeno, il sacrificio da essa imposto nella sfera privata dell'individuo per essere ragionevole deve trovare un adeguato correttivo in norme sufficientemente precise che consentano di limitarne l'incidenza a quanto strettamente necessario (criterio della minima offensività del mezzo). A tal fine, rilevando, oltre ad una differenziazione in ragione dell'obiettivo di lotta contro i reati gravi (o dei fattori di rischio emersi nei riguardi di determinati utenti) [38], l'imprescindibile previsione sia di condizioni sostanziali-procedurali idonee a limitare effettivamente la raccolta e l'utilizzo di tali dati all'esigenza di prevenire un grave rischio per la sicurezza, nonchè di *standard* minimi di garanzia «contro i rischi di abuso [...ed] eventuali [...] usi illeciti dei

[34] Corte giust. UE, Gr. Sez., sent. 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital RightsIreland e Seitlinger e a. contro Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e a.,* §45 ss., in *Dir. pen. cont. - Riv. trim.*, 2014, 2, 178 ss. con nota di Flor.

[35] Così aderendo alle Conclusioni dell'Avv. Gen. UE *Pedro Cruz Villalon*, presentate il 12 dicembre 2013, § 74.

[36] Cfr. Corte giust. UE, Gr. Sez., sent. 8 aprile 2014, cit., punto 27

[37] Cfr. § 74 delle Conclusioni dell'Avv. gen. UE *Pedro Cruz Villalón.*

[38] Come l'esistenza di indizi di natura tale «da far credere che il loro comportamento possa avere un nesso, sia pur indiretto o remoto, con violazioni penali gravi»: cfr. Corte giust. UE, Gr. Sez., sent. 8 aprile 2014, cit., punto 58.

suddetti dati»[39]; sia, segnatamente, di «un previo controllo effettuato da un giudice o da un'entità amministrativa indipendente» cui subordinare l'accesso ai dati conservati[40].

A distanza di meno di due anni, gli approdi raggiunti nella sentenza *Digital Rights* sono stati ribaditi, anche con riguardo alle normative nazionali antecedenti all'invalidata direttiva Frattini e, dunque, estranee all'ambìto applicativo della stessa, nella sentenza *Tele 2 Sverige*[41], alla stregua di una lettura costituzionalmente orientata della direttiva 2002/58/CE (direttiva *e-Privacy*), divenuta l'unica fonte normativa eurounitaria vigente in materia di *data retention*. Statuendosi che la disposizione derogatoria dell'art. 15, par. 1[42], della direttiva *e-Privacy,* mentre è di ostacolo a normative nazionali che, in deroga al divieto di memorizzare i dati di traffico, senza il consenso dell'utente, elevino a regola l'eccezione al principio di riservatezza delle comunicazioni e dei relativi dati di traffico (art. 5, par.1); non osta, invece, ad una conservazione e ad un accesso «mirat[i] dei dati relativi al traffico e dei dati relativi all'ubicazione, per finalità di lotta contro la criminalità grave», allorchè siffatto trattamento sia «limitat[o] allo stretto necessario» per quanto riguarda le categorie dei dati, i mezzi di comunicazione e le persone interessate, nonché la durata di comunicazione[43].

5. *Il mancato adeguamento dello* jus conditum *ai* dicta *della Corte di Lussemburgo.*

Pur non incidendo direttamente sulle normative nazionali di recepimento dell'invalidata direttiva 2006/24/CE, la sentenza *Digital Rights*, di riflesso, ne ha posto in discussione la "tenuta". Così rendendo, da un canto, invalida e, dunque, disapplicabile, da parte dei giudici nazionali, la normativa interna di cui all'art. 132 Codice della *privacy*; e, dall'altro, inutilizzabile l'eventuale atti-

[39] Corte giust. UE, Gr. Sez., sent. 8 aprile 2014, cit., punto 66.

[40] Corte giust. UE, Gr. Sez., sent. 8 aprile 2014, cit., punto 62.

[41] Corte giust. UE, Gr. Sez., sent. 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2 Sverige*AB c. Autorità svedese di Sorveglianza Poste e TLC, in *Dir. pen. cont.,* 9 gennaio 2017, con nota di Pollicino, Bassini.

[42] L'art. 15, par. 1, della Direttiva *e-Privacy* autorizza gli Stati - in deroga all'obbligo di cancellazione o di anonimizzazione dei dati «quando non [...] più necessari ai fini della trasmissione di una comunicazione» (art. 6.1) - ad «adottare norme sulla conservazione di dati da parte dei fornitori dei servizi di comunicazione, per periodi di tempo limitato, allorchè «necessar[i], opportun[i] e proporzionat[i] all'interno di una società democratica per specifici fini di ordine pubblico» .

[43] Corte giust. UE, Gr. Sez., sent. 21 dicembre 2016, cit., punto 108.

vità di *data retention* compiuta fintantoché il legislatore non provvederà ad emendare i relativi profili di contrasto con il diritto primario europeo ([44]).
Per vero, pure l'odierno assetto normativo interno di trasposizione della cd. direttiva Frattini - nella versione risultante dal d.lgs. 30 maggio 2008, n. 109, in parte riformulata dal d.lgs. n. 101 del 2018 - presenta evidenti punti di frizione con il canone di proporzione.
Il regime sistematico ed indiscriminato di archiviazione, istituito dall'art. 132 Codice della *privacy*, con riguardo a tutti i dati di traffico e di ubicazione, a tutti i mezzi di comunicazione elettronica, nonché a tutti gli abbonati e/o utenti registrati, senza limiti o eccezioni di sorta - al di là dell'utopistica differenziazione, operata, da ultimo, sulla base del reato perseguito[45] -, non risulta contemperato da una disciplina sufficientemente precisa sul versante dell'acquisizione dei dati; atteso il *deficit* di determinatezza non solo degli specifici presupposti legittimanti la restrizione della segretezza, ma, anche, delle tipologie di reati gravi cui ancorare l'accesso ai dati stessi. Consentendosi, in virtù del rinvio operato dal co. 3 dell'art. 132 al precedente comma 1, l'accessibilità ai *traffic data*, con decreto motivato del pubblico ministero[46], a prescindere da puntuali criteri oggettivi idonei a limitare il predetto accesso allo stretto necessario - con conseguente automatismo dell'emissione del decreto acquisitivo incompatibile con il criterio del minore sacrificio necessario - e, per di più, per generiche «finalità di accertamento e repressione dei reati»

---

[44] In senso conforme, CRESPI, *Diritti fondamentali, Corte di Giustizia e riforma del sistema UE di protezione dei dati*, in *Riv. it. dir. pubbl. com.*, 2015, 819; IOVENE, Data retention *tra passato e futuro. Ma quale presente?,* in *Cass. pen.,* 2014, 4274; MARCOLINI, *L'istituto della* data retention *dopo la sentenza della Corte di giustizia del 2014,* in *Cybercrime,* diretto da Cadoppi, Canestrari, Manna, Papa, Milano, 2019, 1591ss.; ID., *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen.*, 2015, 760.

[45] V., *infra,* par. 6.

[46] Anche la scelta di esautorare l'organo giurisdizionale dalla procedura di accesso, concentrando in via esclusiva nell'organo di accusa la competenza ad emettere il provvedimento acquisitivo, sembra stridere con gli arresti della Corte di Lussemburgo, oltreché censurabile *ex* artt. 15 e 111 Cost. Sul punto, il nostro, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche,* cit., 120 ss.; in senso critico, pure, FILIPPI, *Intercettazioni, tabulati e altre limitazioni della segretezza delle comunicazioni,* in *Procedura penale. Teoria e pratica del processo,* diretto da Spangher, Marandola, Garuti, Kalb, vol. I, *Soggetti, atti e prove,* a cura di Spangher, Torino, 2015, 977. Da ultimo, analoghe riserve «in ordine all'idoneità del pubblico ministero ad esercitare un controllo preventivo neutro e obiettivo sul carattere proporzionato dell'accesso ai dati», sono state espresse dall'Avv. Gen. UE Giovanni Pitruzzella, nelle conclusioni - presentate il 21 gennaio 2020 - nell'ambito della causa C-746/18, H.K. c. *Prokuratuur*, § 118, con riferimento al diritto estone, tenuto conto dello *status* e dei compiti particolari che ivi distinguono la pubblica accusa dal giudice.

(art. 132, co. 1). Proprio l'estrema indeterminatezza di questo richiamo normativo, del tutto inidoneo – in contrasto non solo con il principio di tassatività, ma pure con il vincolo di scopo - ad individuare le specifiche fattispecie di reato "gravi", in rapporto alle quali delimitare tale accesso, è tale da consentire l'acquisizione dei dati in funzione dell'accertamento di qualsiasi ipotesi di reato, anche contravvenzionale[47].

6. *L'esorbitante innalzamento dei tempi di conservazione dei dati di traffico.*
Dai due *leading cases* in materia, *Digital Rights* e *Tele 2 Sverige*, integranti una sorta di "Statuto europeo" degli strumenti di sorveglianza preposti alla raccolta dei dati esterni ai contenuti delle comunicazioni, il legislatore avrebbe dovuto prendere le mosse sia per un ripensamento dell'istituto, anche sul piano dogmatico - in linea con l'attitudine ad aggredire un'ampia cornice di prerogative individuali, direttamente o indirettamente radicate nella Costituzione (dal diritto alla segretezza sul fatto storico dell'intervenuta comunicazione, al diritto alla tutela della sfera privata e alla protezione dei dati personali)-; sia, altresì, per una meditata revisione organica dell'intera regolamentazione lungo le coordinate segnate dai principi di legalità e proporzione. Per converso, non solo è mancato *in subiecta materia* l'auspicato intervento novellatore di adeguamento agli *standard* europei, ma all'inerzia legislativa hanno fatto da *pendant*, da un canto, soluzioni normative settoriali ad accentuata ispirazione securitaria; dall'altro, antiformalistiche, e fuorvianti, interpretazioni del canone di proporzione, operate dalla giurisprudenza di merito, nell'esercizio di improprie funzioni di supplenza, di poi avallate dalla giurisprudenza legittimità.
Sotto il primo profilo, vengono in rilievo gli interventi di natura eccezionale con cui il legislatore, dietro la spinta della crescente minaccia del terrorismo globale e secondo una ricorrente logica efficientistica del processo, ha innalzato i tempi di conservazione dei dati di traffico telefonico e telematico, in deroga alle cornici temporali fissate dall'art. 132, commi 1 e 1-*bis*, Codice della *privacy*.
Dopo aver previsto, con l'art. 4-*bis* del d.l. 18 febbraio 2015, n. 7, convertito in l. 17 aprile 2015, n. 43, un regime temporaneo di conservazione – fino al 31 dicembre 2016, di poi prorogato fino al 30 giugno 2017 – dei dati di traffico, per le finalità di accertamento e repressione dei reati di cui agli artt. 51,

[47]Proprio sotto questo profilo è stata prospettata l'incompatibilità, con gli artt. 7, 8 e 52 par. 1 CDFUE, dell'art. 132 Codice della *privacy:* sul punto, v., *infra*, par. 7.

co. 3-*quater,* e 407, co. 2, lett. *a)*, c.p.p., si è pervenuti, in assenza di un nuovo provvedimento di proroga, ad un significativo, e quanto mai preoccupante, prolungamento dei tempi di conservazione in evidente attrito con il canone di proporzione. Per vero, in attuazione dell'art. 20 della direttiva 2017/541, sulla lotta contro il terrorismo (sostitutiva della decisione quadro 2002/475/GAI), il nostro legislatore è intervenuto, con l'art. 24 della legge europea 20 novembre 2017, n. 167, al fine «di garantire strumenti di indagine efficace in considerazione delle straordinarie esigenze di contrasto del terrorismo, anche internazionale, per le finalità dell'accertamento e della repressione dei reati dei reati di cui all'art. 51 co. 3-*quater,* e 407, co. 2, lett. *a)*, [c.p.p.]», fissando il termine di *retention* dei dati telefonici-telematici (nonché dei tentativi di chiamate non risposte) in settantadue mesi (pari a sei anni!). Detto regime, concepito, in origine, in un'ottica emergenziale ed eccezionale, è divenuto ordinario, essendo stato trasfuso nel nuovo comma 5-*bis* dell'art. 132 Codice della *privacy* - interpolato dall'art. 11 del d.lgs. n. 101 del 2018 - che ha«fatt[o] salva la disciplina di cui all'art. 24 della legge 20 novembre 2017, n. 167». Intenzione del legislatore era quella di introdurre un regime binario di conservazione-acquisizione, differenziato sulla base del reato perseguito. Rinviandosi, per i reati comuni, all'articolata tempistica - di ventiquattro mesi, di dodici mesi e di trenta giorni - prevista dal citato art. 132, co. 1 e 1-*bis*, di cui si è supposta maldestramente la vigenza nonostante la contrarietà con il diritto UE[48]; e prevedendosi, per la criminalità grave di stampo terroristico, un termine omogeneo di conservazione pari a settantadue mesi, a prescindere dalla provenienza dei dati trattati. Siffatta divaricazione dei tempi di conservazione dei dati di traffico non è, però, attuabile sul piano concreto[49]. Per vero, il gestore - gravato di oneri esorbitanti le sue competenze - non potendo sapere *ex ante* per quale tipologia di reati i dati verranno, ipoteticamente, richiesti dal pubblico ministero, sarà obbligato a conservare la considerevole mole di dati generati dalle comunicazioni (via telefono, da Internet o dalle chiamate senza risposta) per il periodo di sei anni. È, semmai, nel momento in cui il pubblico ministero ne richiederà l'acquisizione che la diversa tempistica temporale potrà as-

[48] Critico sul punto è pure MARCOLINI, *L'istituto della* data retention *dopo la sentenza della Corte di giustizia del 2014,* cit., 1593.

[49] Come è stato, da subito, posto in rilievo in dottrina: cfr. SIGNORATO, *Novità in tema di Data retention. La riformulazione dell'art. 132 Codice Privacy da parte del d.lgs. 10 agosto 2018, n.* 101, in *Dir. pen. cont.,* 2018, 11, 156 ss.; conf. BACCARI, *Il trattamento (anche elettronico) dei dati personali per finalità di accertamento dei reati,* in *Cybercrime,* diretto da Cadoppi, Canestrari, Manna, Papa, Milano, 2019, 1610.

sumere un qualche rilievo; dovendosi indicare, da parte dell'autorità giudiziaria, nel relativo decreto acquisitivo, la specifica tipologia di reato per il quale si stia procedendo. Con la conseguenza che, là dove la richiesta, riguardante, per ipotesi, dati telefonici da conservare per due anni e finalizzata, dunque, a perseguire reati comuni, fosse presentata alla scadenza del termine di ventiquattro mesi, dovrebbe ritenersi illegittima l'acquisizione ed inutilizzabili i relativi dati, atteso il divieto di conservazione dei dati stessi da parte del gestore oltre il periodo normativamente predeterminato.

Orbene, se, dunque, alla stregua del combinato disposto dei commi 1, 1-*bis* e 5-*bis* dell'art. 132 Codice della *privacy*, i tempi ordinari di conservazione dei dati telefonici-telematici si sono ormai assestati in sei anni, allora non può revocarsi in dubbio come, anche sotto questo profilo, il nostro assetto normativo non sia esente da serie censure di incompatibilità con il diritto eurounitario. Si tratta, infatti, di un termine unitario di cancellazione palesemente non "adeguato", in contrasto con l'art. 5 della direttiva 2016/680[50], e lesivo del diritto all'oblìo[51], oltrechè esorbitante il limite di stretta necessità[52] in cui si declina il canone di proporzione[53].

7. *La ricostruzione "deformante" del* proportionality check *nella giurisprudenza nazionale.*

Il silenzio serbato dal legislatore in ordine alla soglia di sufficiente gravità dei reati presupposto - criterio su cui si misura il rispetto del principio di propor-

---

[50] L'art. 5 (Termini di conservazione ed esame) della direttiva 2016/680 prescrive l'obbligo degli Stati di fissare «adeguati termini per la cancellazione dei dati personali».

[51] *Id est,* della pretesa - ricompresa nella più ampia garanzia di *habeas data* e sancita espressamente dall'art. 17 del Regolamento 2016/679 - dell'interessato di ottenere «senza giustificato ritardo», da parte del titolare del trattamento, la cancellazione dei dati personali che lo riguardano.

[52] ...evocato, con specifico riguardo al momento della conservazione dei dati personali, dall'art. 4, par. 1, lett. *d),* della direttiva 2016/680, ai sensi del quale i dati sono «conservati [...] per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati»; cui corrisponde l'art. 3, par. 1, lett. *a)* del d.lgs. n. 51/ 2018, attuativo della direttiva stessa, che prevede che i dati personali siano «conservati [...] per il tempo necessario al conseguimento delle finalità per le quali sono trattati, [...], cancellati o anonimizzati una volta decorso tale termine».

[53] Ad analogo rapporto "squilibrato" tra *privacy* e sicurezza, in contrasto con il modello forte di protezione dei dati personali recepito dal diritto Ue, è improntata pure la tempistica di conservazione dei dati personali, oggetto di trattamento da parte delle forze di polizia giudiziaria, di cui all'art. 10, co. 3, del d.p.r. del 15 gennaio 2018, n. 15. Prevedendosi termini differenziati, in base al provvedimento adottato, che vanno dai 18 mesi ai 30 anni (in senso critico, GALGANI, *Giudizio penale,* habeas data *e garanzie fondamentali*, in *questa Rivista*, 2019, 1).

zionalità che giustifica l'ingerenza, implicata dalla *data retention*, nei diritti fondamentali di cui agli artt. 7 e 8 CDFUE - ha finito per "scaricare" sull'autorità giudiziaria il compito di tracciare, di volta in volta, la linea di confine tra reati gravi e non. Così da delegare, in ultima analisi, alla valutazione, inevitabilmente arbitraria e contingente di quest'ultima, il delicato bilanciamento tra *auctoritas e libertas*, ovvero l'individuazione di quel ragionevole punto di equilibrio, tra le diverse esigenze in gioco, idoneo a salvaguardare il contenuto essenziale dei diritti fondamentali.

Per vero, il giudice di merito, intervenuto sulla prospettata incompatibilità dell'art. 132 Codice della *privacy* con gli artt. 7, 8 e 52 par. 1 CDFUE, sotto il profilo relativo all'omessa previsione di uno specifico catalogo di reati sufficientemente gravi, ha preteso di sanarne il contrasto sostituendosi al legislatore nella valutazione di gravità del reato oggetto del procedimento, così da giustificare l'avvenuta acquisizione dei dati relativi al traffico a fini investigativi[54].

Dal canto suo, la giurisprudenza di legittimità, dinanzi alla quale è stata più volte sollevata la relativa questione, ha perso l'occasione - seppur obbligata, *ex* art. 267 TFUE, in qualità di organo giurisdizionale di ultima istanza - per interpellare i Giudici di Lussemburgo sulla compatibilità della normativa interna con la Carta dei diritti UE; asserendosi che i principi enunciati nelle sentenze *Digital Rights* e *Tele 2 Sverige* riguarderebbero i soli Stati UE privi di una regolamentazione in materia di *data retention* e non avrebbero un particolare impatto sull'art. 132 Codice della *privacy*[55].

Più nello specifico, secondo l'orientamento della giurisprudenza consolidata, la disciplina nazionale, sebbene non limiti l'accesso ai dati di traffico telefonico, a fini di giustizia penale, a categorie di reati ritenuti particolarmente gravi, non sarebbe in contrasto con la disciplina sovranazionale; il cui rispetto imporrebbe solo un vaglio in concreto della proporzione tra gravità dell'ingerenza nel diritto fondamentale alla vita privata, che l'accesso ai dati comporta, e

[54] Cfr. Trib. Padova, ord. 15 marzo 2017, Pres. Marassi – in *www.penalecontemporaneo.it*, con nota di Flor, e in *Cass. pen.,* 2017, 2483 ss., con nota di Ruggieri - che ha rigettato l'eccezione di inutilizzabilità in relazione ai dati esterni del traffico telefonico acquisiti *ex* art. 132 del Codice della *privacy*, nonché la richiesta, *in subordine*, di sospendere *ex* art. 267 TFUE il procedimento e sottoporre la relativa questione pregiudiziale alla Corte di giustizia sulla base di una serie di elementi argomentativi erronei, tra cui l'asserita osservanza in concreto del principio di proporzionalità, attesa l'acquisizione dei dati ai fini dell'accertamento di un reato – il tentato incendio doloso aggravato – ritenuto dallo stesso giudice di gravità tale da consentire l'ingerenza nel diritto alla *privacy*.

[55] In tal senso, Cass., Sez. III, 25 settembre 2019, Riccio Clemenz, *non massimata*; conf. Cass., Sez. III, 19 aprile 2019, D'Addiego, in *www.sistemapenale.it*, con nota di NERONI REZENDE; Cass., Sez. V, 24 aprile 2018, M., in *Cass. pen.*, 2019, 299.

gravità del reato oggetto d'indagine.
Una valutazione che, secondo detto indirizzo ermeneutico,«dipende[ndo] da una serie di variabili connesse alla particolarità dei casi concreti, mal si presta ad una preventiva, rigida, codificazione e non può che essere rimessa al prudente apprezzamento dell'autorità giudiziaria, o comunque indipendente, che per la normativa eurounitaria[...]costituisce indefettibile garanzia rispetto alla tutela dei diritti fondamentali». Con la conseguenza che, laddove nel successivo giudizio si contesti la legittima acquisizione di tali dati, sarebbe compito del giudice «verificare se il menzionato requisito di proporzione possa dirsi soddisfatto al fine di ritenere o negare l'utilizzabilità processuale dei dati medesimi ai sensi dell'art. 191 c.p.p.». E, ulteriormente, sottolineandosi che la mancata indicazione, nell'art. 132 Codice della *privacy*, di parametri cui informare il suddetto giudizio di proporzionalità non rischierebbe di renderlo arbitrario, poichè dalla legislazione processuale sarebbero ricavabili utili criteri, venendo in particolar modo in rilievo, la previsione contenuta nell'art. 266 c.p.p., comma 1, lett. *a)*, che, modulata sulla minore invasività della raccolta dei *traffic data* rispetto alle intercettazioni, dovrebbe consentire quest'attività per reati puniti meno gravemente[56].
Si tratta, all'evidenza, di un approccio ermeneutico riduttivo, che non coglie la piena accezione del canone di proporzione, trascurandone la duplice dimensione (astratta e pratica) che lo contraddistingue[57]. Indirizzandosi, detto canone, in prima battuta, al legislatore, quale ineludibile limite razionale-contenutistico delle scelte discrezionali inerenti la determinazione dei casi e dei modi di aggressione di un diritto inviolabile dell'uomo; e, in un secondo momento, all'autorità giudiziaria, in sede di adozione del provvedimento restrittivo o di verifica della legittimità del bilanciamento concreto operato da tale provvedimento.
In ossequio a questo criterio guida, non basta la puntuale regolamentazione normativa dell'ingerenza; occorrendo, altresì, la previsione di parametri e garanzie idonee a contenere l'ingerenza stessa entro l'orizzonte di limite, segnato dal triplice *standard* di giudizio in cui detto criterio si articola (idoneità, minima offensività e proporzionalità in senso stretto).
Né può, d'altro canto, dubitarsi della vincolatività del canone di proporzione.

---

[56] Cfr. Cass., Sez. III, 25 settembre 2019, Riccio Clemenz, cit.

[57] Critico nei confronti di tale approccio dei nostri giudici, i quali mostrano scarsa sensibilità e non piena consapevolezza circa i caratteri strutturali del canone di proporzione è NICOLICCHIA, *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni rispetto ai nuovi mezzi di ricerca della prova,* in *www.penalecontemporaneo.it.*

Già enucleato dalla Corte di Strasburgo dal limite di «necessità» di cui all'art. 8, par. 2, CEDU, detto canone dispiega la sua forza vincolante nell'intero sistema (penale e processuale)[58], essendo ormai formalizzato, nell'art. 52, par. 1, CDFUE, quale principio generale dell'assetto costituzionale dell'Unione quale "Comunità di diritti"; trovando, altresì, espressione nel principio della cd. minimizzazione dei dati, oggetto del trattamento, di cui agli artt. 5, par. 1, lett. *c)*, del GDPR e 4, par. 1, lett. *c)* della direttiva UE 2016/680[59].
Invece, secondo la ricostruzione interpretativa recepita dalla giurisprudenza di legittimità, l'autorità giudiziaria, cui spetterebbe il compito di vagliare in concreto la proporzionalità tra gravità dell'ingerenza e gravità del reato, sulla sola base delle peculiarità del caso e, dunque, anche a prescindere da limiti normativi, potrebbe, altresì, sostituirsi al legislatore nella determinazione della soglia di sufficiente gravità dei reati-presupposto idonea a legittimare l'acquisizione dei dati. Supplendo, in tal modo, alle lacune della normativa interna, ma con esiti applicativi arbitrari e confliggenti con il principio di legalità processuale, che rischiano di trasformare lo scrutinio di proporzionalità in uno strumento interpretativo utilizzabile *ex post* per giustificare di volta in volta la violazione dei diritti fondamentali[60].

8. *Segue: il diritto vivente eurounitario*. Un approccio fuorviante al canone di proporzione che non trova affatto riscontro, come erroneamente asserito[61], nella più recente giurisprudenza della Corte di Lussemburgo, successiva alle sentenze *Digital Rights* e *Tele 2Sverige.*

---

[58] Si tratta, peraltro, di un principio tutt'altro che nuovo nel nostro ordinamento, improntando l'intera area dei diritti inviolabili garantiti dalla Costituzione: cfr. CAIANELLO, *Il principio di proporzionalità nel procedimento penale,* in *Dir. pen. cont. -Riv.trim.,* 2014, 3-4, 148 e, volendo, il nostro, *L'acquisizione nel processo penale dei dati esteriori delle comunicazioni telefoniche e telematiche*, cit., 78 ss.

[59] L'art. 5, par. 1, lett. *c*), GDPR (Principi applicabili al trattamento dei dati personali) – e, in termini analoghi, il corrispondente art. 4, par. 1, lett. *c,)* della direttiva (UE) 2016/680 del 27 aprile 2016– prescrive che i dati, oggetto del trattamento, siano «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali siano trattati (cd. minimizzazione dei dati)». E, in modo del tutto simmetrico, l'art. 3, par. 1, lett. *c)* del d.lgs. 2018, n. 51, prevede che i dati personali siano «adeguati, pertinenti e non eccedenti rispetto alle finalità per quali sono trattati».

[60] Conf. NICOLICCHIA, *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni rispetto ai nuovi mezzi di ricerca della prova*, cit. Con specifico riguardo all'ordine europeo di indagine penale di cui alla direttiva 2014/41/UE, le derive antiformalistiche della giurisprudenza di legittimità vengono stigmatizzate da UBERTIS, *Equità e proporzionalità* versus *legalità processuale: eterogenesi dei fini?*, in *questa Rivista*, 2017, 2, 3.

[61] Cfr. Cass., Sez. III, 25 settembre 2019, n. 48737, Riccio Clemenz, cit., punti 3.6 e 3.7.

A seguito della declaratoria d'invalidità della direttiva 2006/24/CE, la diversità di approcci normativi adottati dagli Stati membri in materia di *data retention*, nonché la vaghezza del dato letterale dell'art. 15 della direttiva *e-Privacy*, che - con riguardo alle specifiche finalità investigative che giustificano l'adozione di misure nazionali derogatorie - richiama i reati in generale (e non i soli reati gravi), hanno dato origine a molteplici controversie alcune delle quali ancora pendenti. Offrendo, alla Corte di giustizia UE, l'occasione per definire i limiti entro i quali le autorità nazionali possono acquisire i *traffic data* conservati dai *provider* di servizi di telefonìa e, dunque, i termini del delicato bilanciamento tra tutela della *privacy*, da un canto, e *data retention* per finalità di sicurezza, dall'altro.

I Giudici di Lussemburgo si sono, comunque, limitati a precisare il perimetro applicativo del citato art. 15, chiarendone il contenuto precettivo, senza, però, mettere in discussione gli approdi dei due *leading cases* in materia e, anzi, proseguendo il percorso di rilettura costituzionale della normativa di diritto derivato già avviato dalla sentenza *Tele2 Sverige.* Emblematica in tal senso, è la decisione assunta nella causa Ministerio *Fiscal*, in cui la Corte di giustizia UE, è stata investita dal giudice spagnolo, *l'Audiencia Provincial de Tarragona*, della questione pregiudiziale relativa alla compatibilità con l'art. 15, par. 1, della direttiva *e-Privacy* - letto alla luce degli artt. 7, 8, 11 e 52, par. 1, CDFUE - di una normativa nazionale che prevede l'accesso da parte delle autorità competenti, la polizia giudiziaria, ai soli dati che mirano all'identificazione dei titolari di carte SIM attivate con un telefono cellulare rubato, come il cognome, il nome e, se del caso, l'indirizzo di tali titolari[62]. Ivi, muovendo dalle conclusioni della sentenza *Tele2Sverige*, i Giudici di Lussemburgo si sono premurati di operare i dovuti distinguo tra l'ingerenza oggetto del procedimento e quella considerata nella pronuncia *Tele2 Sverige.* Sottolineandosi l'esigenza di calibrare la valutazione relativa al grado di ingerenza nei diritti fondamentali, derivante dall'accesso ai dati relativi al traffico, in rapporto ad una serie di variabili correlate sia alla tipologia di dati che vengono in rilievo,

[62] Corte giust. UE, Gr. Sez., sent. 2 ottobre 2018, causa C-207/16, *Ministerio Fiscal.* Più nel dettaglio, il giudice di rinvio chiedeva, con le sue due questioni, se l'art. 15, par. 1, della direttiva 2002/58/CE, dovesse essere interpretato nel senso che l'accesso delle autorità ai dati in questione comportasse un'ingerenza nei diritti fondamentali sanciti dalla Carta, che presentasse una gravità tale da dover limitare il suddetto accesso, in materia di prevenzione, accertamento e perseguimento dei reati, alla lotta contro la criminalità grave e, in caso affermativo, sulla base di quali criteri dovesse essere valutata la gravità dell'infrazione in questione.

sia alla portata delle operazioni di accesso - circoscritta o estesa ad un ampio ventaglio di dati -, sia alla durata del periodo temporale per cui sono richiesti i dati.

Nel suo *reasoning* la Corte di giustizia UE, richiamata la necessità di una corrispondenza tra il grado dell'ingerenza e l'obiettivo perseguito dalla normativa che regola tale raccolta, ha sottolineato che, in conformità al principio di proporzionalità, soltanto la lotta contro la criminalità "grave" è idonea a condizionare, e giustificare, una grave ingerenza, come quella conseguente «[all']accesso delle autorità pubbliche a dati personali conservati dai fornitori di servizi di comunicazione che, considerati nel loro insieme, consentono di trarre conclusioni precise sulla vita privata delle persone i cui dati sono oggetto di attenzione»[63]. Al contrario, «qualora l'ingerenza che comporta tale accesso non sia grave, [lo stesso] può essere giustificato da un obiettivo di prevenzione, ricerca, accertamento e perseguimento di un "reato" in generale»[64].

Deducendosi da tali rilievi che l'acquisizione dei soli dati oggetto della domanda in questione, una ristretta tipologia di dati - ovvero solo quelli identificativi del soggetto titolare della carta SIM - per di più, relativa ad un periodo di tempo limitato a dodici giorni, non può qualificarsi come un'ingerenza "grave" nei diritti fondamentali della persona; atteso che «senza una verifica incrociata dei dati relativi alle comunicazioni effettuate con tali schede SIM e dei dati relativi all'ubicazione, questi dati non permettono di conoscere né la data, né l'ora, né la durata, né i destinatari delle comunicazioni effettuate con [lao] le carte[...] in questione, né i luoghi in cui dette comunicazioni sono avvenute o la frequenza di esse con talune persone nel corso di un determinato periodo»[65]. Di talchè, non consentendo di trarre conclusioni precise sulla vita privata delle persone, l'accesso ai dati relativi all'identità civile dei titolari delle schede SIM non deve essere sorretto da una giustificazione rafforzata, potendo essere autorizzato pure ai fini della prevenzione, ricerca, accertamento e perseguimento di un reato in generale, anche non grave.

Si è, così, confermata, implicitamente, lungo i binari esegetici già tracciati nella sentenza *Tele2 Sverige*, l'illegittimità di tutte quelle normative nazionali, come quella tutt'ora recepita dall'art. 132 Codice della *privacy*, che prevedano, in relazione a qualsiasi fattispecie di reato, la conservazione ed acquisizione *a posteriori*, da parte delle autorità competenti, della mole indiscriminata

[63] Corte giust. UE, Gr. Sez., sent. 2 ottobre 2018, causa C-207/16, cit., punto 41 (che richiama il punto 99 della sentenza relativa al caso Tele 2 Sverige e Watson e a.).

[64] Corte giust. UE, Gr. Sez., sent. 2 ottobre 2018, cit., punto 44.

[65] Corte giust. UE, Gr. Sez., sent. 2 ottobre 2018, cit., punto 48.

di informazioni - contenute nei tabulati - relative al traffico telefonico (o telematico) già intercorso in un determinato apparecchio. Sconfessandosi, quindi, l'interpretazione *soft*, recepita dalla nostra giurisprudenza, secondo cui la disciplina sovranazionale di matrice eurounitaria, come interpretata dal diritto vivente, consentirebbe, fatta salva la valutazione in concreto del rispetto del principio di proporzionalità, l'accesso, a fini di giustizia penale, ai dati relativi al traffico quale che sia la gravità dei reati[66]. In linea di continuità si pone, pure, un'altra causa di rilievo che, a breve, verrà decisa dai Giudici di Lussemburgo (causa C-746/18, H.K. c. *Prokuratuur*), attinente al medesimo profilo relativo alle condizioni di accesso ai *traffic data*; essendo stato posto, dalla Corte suprema dell'Estonia, il quesito se l'art. 15, par. 1, della direttiva 2002/58/CE, letto in aderenza alla Carta dei diritti fondamentali UE, debba essere interpretato nel senso che tra i criteri rilevanti,ai fini della valutazione della gravità dell'ingerenza nei diritti fondamentali, rientri, oltre alle categorie di dati, anche la durata del periodo con riferimento al quale l'accesso è richiesto. È assai probabile che, in coerenza con quanto già anticipato nel caso *Ministerio Fiscal*, i Giudici di Lussemburgo daranno risposta positiva al quesito, aderendo così alle conclusioni dell'Avvocato generale; il quale ha posto in rilievo come la lettura combinata della «natura dei dati considerati e [del]la durata del periodo oggetto dell'accesso» consenta di verificare se risulti soddisfatto il criterio decisivo per la gravità dell'ingerenza, «ossia se l'accesso ai dati di cui trattasi possa permettere alle autorità nazionali competenti di trarre conclusioni precise riguardo alla vita privata delle persone i cui dati sono interessati da tale accesso»[67]. Pervenendosi alla condivisibile conclusione che, laddove la combinazione di tali due aspetti non permetta di delineare il preciso ritratto di una persona, l'autorità giudiziaria possa accedere ai metadati delle comunicazioni elettroniche anche per il perseguimento di reati non gravi. Dall'analisi degli approdi del diritto vivente eurounitario, successivi alla sentenza *Digital rights*, emerge, in definitiva, come, attraverso l'esegesi ricostruttiva in chiave costituzionale dei contenuti precettivi dell'art. 15 della direttiva *e-Privacy*, sia in atto la progressiva statuizione, ad opera della Corte di giustizia UE, dei principi normativi, alla stregua dei quali contemperare, *in subiecta*

[66] Cfr. Cass., Sez. III, 25 settembre 2019, Riccio Clemenz, cit., punti 3.6 e 3.7.

[67] Conclusioni dell'Avv. Gen. UE Giovanni Pitruzzella, causa C-746/18, H.K. c. *Prokuratuur*, cit., §82, in cui si precisa come «per poter delineare il preciso ritratto di una persona [sia] necessario non soltanto che l'accesso riguardi più categorie di dati, come i dati identificativi, relativi al traffico e i dati relativi all'ubicazione, ma anche che tale accesso abbia ad oggetto un periodo abbastanza lungo da poter rivelare con sufficiente precisione gli aspetti principali della vita di una persona».

materia, il binomio *privacy*-sicurezza; e destinati non solo a trovare applicazione da parte dei giudici nazionali, ma anche a influenzare i futuri sviluppi normativi a livello sovranazionale[68], in quel complesso intreccio tra fonti normative e giurisprudenza fonte che caratterizza il diritto europeo[69].

[68] Si fa riferimento, in particolare, ai negoziati in corso riguardanti il Regolamento e*Privacy*, relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche; che sostituirà la Direttiva 2002/54/CE, estendendone il campo di applicazione a tutti i fornitori di comunicazioni elettroniche - inclusi i cd. servizi "*over-the-top*" - nell'intento di garantire, in vista del mercato unico digitale, un elevato livello di riservatezza per tutti gli operatori di mercato (v. la bozza del Regolamento del Parlamento europeo e del Consiglio, presentata dalla Commissione europea nel gennaio 2017 COM (2017) 10 final 2017/0003).

[69] Di talchè la normativa in tema di *data retention*, in quanto prodotto del diritto europeo nel significato concreto che le è conferito dalla Corte di giustizia UE, appare veramente paradigmatica della «transizione» ad una legalità europea, a natura ibrida (cfr. VOGLIOTTI, *La nuova legalità penale, il ruolo della giurisprudenza. Spunti per un confronto*, in *Sist. pen.*, 2020, 3, 60 ss.; e, già, ID., voce *Legalità*, in *Enc. dir. Annali*, VI, Milano, 2013, 410 ss.), «di tipo "dinamico" prevalentemente giudiziale» (cfr. KOSTORIS, *Processo penale, diritto europeo e nuovi paradigmi del pluralismo giuridico postmoderno,* in *Riv. it. dir. proc. pen.*, 2015, 3, 1177ss.), incentrata su parametri di razionalità pratica ed incline a valorizzare le esigenze di adeguatezza, necessità e proporzionalità dell'intervento.