GIOIA SAMBUCO

Note in tema di *data retention*

Nella magmatica ed attuale disciplina della *data retention*, la Corte UE ha ribadito -anche recentemente con la pronuncia C-140/20 del 5.4.2022- come i dati di traffico siano sempre idonei, in quanto tali, a trarre precise conclusioni sulla vita privata dei cittadini, a prescindere dalla durata del periodo per il quale l'accesso ai suddetti viene richiesto, nonché dalla quantità o dalla natura dei dati disponibili per tale periodo. Le pronunce rese in argomento dai giudici di Lussemburgo costituiscono un esempio di contemperamento tra diritti fondamentali; purtuttavia la la tutela della protezione dei dati nella UE non è lasciata alla sola azione di controllo della Corte di giustizia, ma lo stesso legislatore europeo, gradatamente, ha costruito un quadro normativo di protezione, completo ed adeguato –il più possibile- alle nuove esigenze del sistema internazionale che ogni legislatore nazionale è chiamato efficacemente a garantire e, nel caso, adeguatamente ad implementare.

Notes on data retention

In the current, magmatic discipline on data retention, the EU Court reiterated - recently, with the judgment C-140/20 deliverd on 5 April 2020 – that traffic data are always suitable to draw precise conclusions on private life of citizens, regardless of the length of the period for which the access to the system is required or regardless of the quantity or the nature of the available data for the period. The judgment of the Luxemburg Court constitute an example of a balance between fundamental rights; however the data protection in EU is not subject only to the control of the Court, but the European legislator, gradually, has built a regulatory framework of protection, able to respect the new requirements of the international system that every national legislator is called upon to effectively guarantee and, if necessary, to adequately implement.

1. *Premessa.* La recente pronuncia C-140/20 resa in data 5 aprile 2022, dalla Corte di giustizia UE offre lo spunto per la disamina del contesto normativo e della prassi giurisprudenziale in tema di *data retention* volendo riferirsi, con questa espressione, precisamente, alla conservazione di dati relativi al traffico, ovvero a quei dati sottoposti «*a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica*»[1].

[1] Così art. 2, 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, in *Gazz. Uff. CE*, 31 luglio 2002, L. 201, 37. Cfr. *infra* nonché per un maggiore approfondimento del contesto normativo e della prassi giurisprudenziale della Corte di Lussemburgo NINO, *L'annullamento del regime della conservazione dei dati di traffico nell'Unione europea da parte della Corte di giustizia UE: prospettive ed evoluzioni future del sistema europeo di data retention,* in *Dir. un. europea, 2014, 4, 803,* nonché FLOR, *Dalla data retention al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di giustizia. Quali effetti per il sistema di giustizia penale e quali pro-*

Pur non essendo possibile, dai dati *de quibus,* apprendere il contenuto di una comunicazione, comunque, questi, consentono di ottenere informazioni sulla vita privata di una persona, creare profili della sua personalità, tracciarne i movimenti, talvolta ingenerando l'impressione di vivere in una società a tutti gli effetti sorvegliata. Ed infatti da una serie di dati quali: data, luogo, orario di una comunicazione, siti *Internet* visitati, chiamate in entrate ed in uscita, ove combinati tra loro, è possibile finanche ricavare dettagliate informazioni (a titolo esemplificativo: sugli orientamenti religiosi, sull'appartenenza a gruppi politici o associazioni sindacali, sulle relazioni sociali o sulle inclinazioni personali ecc.).
Siffatta attività costituisce, indubbiamente, uno strumento particolarmente utile nella lotta al terrorismo ed alla criminalità organizzata, potendo agevolare le autorità di *intelligence* e di polizia nell'espletamento delle indagini per la prevenzione e repressione di reati gravi; è però innegabile che questa, ingeneri, appunto indubbiamente, una serie di problematiche sotto il profilo della sua conformità o meno ai principi internazionali ed europei in materia di protezione dei dati, quali, a titolo esemplificativo, i principi di necessità, finalità limitata e proporzionalità dei dati stessi[2]: difatti, si anticipa sin da subito, in spregio a questi ultimi, la *data retention* costituirebbe una ingerenza grave ed ingiustificata nella vita privata degli individui sottoposti alla "sorveglianza".

2. *Quadro di riferimento.* Da oramai un decennio è stata assegnata, ai Giudici di Lussembrugo, una "nuova" funzione: garantire una più penetrante tutela dei diritti fondamentali dei cittadini avverso le iniziative delle istituzioni europee, degli Stati nonché del paese di cittadinanza[3]; la Corte di giusitizia, infatti,

---

spettive de jure condendo?, in *Dir. informaz. e informatica*, 2014, 4-5. 775.

[2] Con particolare riferimento al principio di proporzionalità, espressamente richiamato -come è noto- nel codice di rito in materia di misure cautelari personali (art. 275 c.p.p.), v'è da chiarire come questo costituisca un vero e proprio principio generale dell'intero sistema processuale penale, destinato a venire in rilievo a fronte di attività limitative dei diritti fondamentali della persona, tra cui *in primis* i mezzi di ricerca della prova. Ciò deve, pertanto, valere anche con riferimento alla conservazione e acquisizione dei dati di traffico. Né si potrebbero ricavare indicazioni di segno contrario, come di qui a breve si dirà *infra*, dalla circostanza che la relativa disciplina è contenuta nel Codice *privacy* e non in quello di rito. Infatti, la suddetta collocazione non vale, in ogni caso, a sottrarre un'attività assimilabile ai mezzi di ricerca della prova, ai principi fondamentali che governano la materia. Per riflessioni in argomento cfr. ORLANDI, *Garanzie individuali ed esigenze repressive (ragionando intorno al diritto di difesa nei procedimenti di criminalità organizzata*), in *Studi in ricordo di G. Pisapia. Procedura penale* II, Milano, 2000, 560 nonché CAIANIELLO, *Il principio di proporzionalità nel procedimento penale,* in *Dir. pen. cont.*, 18 giugno 2014.

[3] In argomento v. TIZZANO, *Qualche riflessione sul contributo della Corte di giustizia allo sviluppo del sistema comunitario*, in *Nuovi strumenti di diritto internazionale privato*, a cura di Bariatti - Venturini,

ha assunto il ruolo (e, conseguentemente, la responsabilità) di giudice dei diritti fondamentali che, concretamente, esercita principalmente nei giudizi di cui agli articoli 256, 263 e 267 TFUE[4].

D'altra parte, i diritti fondamentali UE, al pari peraltro di quelli sanciti nella CEDU, possono soggiacere a vere e proprie restrizioni che, ai sensi dell'articolo 52.1 della Carta, devono essere previste dalla legge, proporzionate, necessarie, nonché devono rispettare il contenuto essenziale di detti diritti e libertà e rispondere a finalità d'interesse generale riconosciute dall'Unione od all'esigenza di proteggere i diritti e le libertà altrui[5].

Proprio le pronunce rese in tema di protezione dei dati personali, argomento, questo, che sta assumendo sempre più impulso[6], costituiscono un recente esempio di contemperamento tra diritti fondamentali.

Del resto, ciò è inevitabile: la maggior attenzione, anche a livello sovranazionale, alla protezione dei dati è, obiettivamente comprensibile in ragione del fatto, *in primis,* che l'uso, sempre più frequente di *Internet* per comunicare, avere accesso e scambiare informazioni, oltrechè per offrire ed acquistare beni o servizi, espone la vita privata degli individui a nuovi e sempre maggiori rischi.

In ordine a questo profilo, senza timore di smentita, può sostenersi come, oramai, la circolazione dei dati sia, diventata a tutti gli effetti "internazionale"[7]

Milano, 2009, 925. Sul punto v. altresì IOVENE, *Data retention tra passato e futuro. Ma quale presente?,* in *Cass. pen.*, 2014, 12, 4274. In argomento v'è altresì da segnalare come, parte della dottrina, ormai da tempo, ritiene che l'UE sia «esportatrice di diritto». Così, per tutti, LAÏDI, *La norme sans la force: l'énigme de la puissance européenne*, Paris, 2014, *passim.*

[4] L'articolo 47 della Carta UE assicura, in favore di ciascun cittadino i cui diritti e le cui libertà egli pretenda essere stati violati il diritto ad un ricorso effettivo, davanti ai giudici (oltreché nazionali) anche dell'UE. Per un approfondimento del disposto normativo in discorso, non soltanto in riferimento al diritto di accesso alla giustizia ma alla stessa nozione di "giustizia" (intesa come procedimento giurisdizionale) e al connesso diritto a farsi rappresentare, v. ALPA, *Il diritto fondamentale ad un rimedio effettivo e il ruolo costituzionale dell'avvocato*, reperibile *on line* sul sito *www.consiglionazionaleforense.it.*

[5] Invero, l'analisi della giurisprudenza antecedente il Trattato di Lisbona mostra come i giudici di Lussemburgo non abbiano esitato a condizionare l'esercizio anche delle libertà di circolazione, pietra angolare del sistema comune; in argomento v. ampiamente CRESPI, *Rivista Italiana di Diritto Pubblico Comunitario*, 3-4, 2015, 819.

[6] In tale ambito, sin dal 2014, il giudice di Lussemburgo è stato ripetutamente chiamato a pronunciarsi sul valore del diritto dei privati alla protezione dei dati personali; note, al riguardo, le sentenze *Google Spagna* e *Digital Rights Irland Ltd* nelle quali, la Corte di giustizia è stata chiamata a scrutinare siffatto diritto rispetto agli altri diritti fondamentali (quali quello d'autore, iniziativa economica, libertà d'informazione e d'espressione, pubblica sicurezza), nonché nei rapporti tanto tra persone fisiche e giuridiche quanto tra cittadini e autorità pubbliche. Così, rispettivamente: Corte giust. UE, 6 novembre 2003, C-101/01, Lindqvist; Corte giust. UE, 13 maggio 2014, C-131/12.

[7] Condivisibile quanto sostenuto secondo cui «Mediante l'uso della tecnologia, il dato valica anche i confini dell'internazionale e diventa sovranazionale», in questi termini: SCARCHILLO, *Il trasferimento di*

e, anche per ciò solo, presupporrebbe una efficace tutela comune.
Inoltre, la protezione dei dati è espressamente menzionata nel diritto primario e, in particolare, nella Carta quale diritto fondamentale (articolo 8.2)[8] peraltro autonomo rispetto al diritto alla vita privata e familiare di cui all'articolo 7[9] nonché *sub* art. 16 par. 1 del Trattato sul funzionamento dell'Unione europea[10]; conseguentemente le istituzioni dell'Unione europea sono chiamate a fare rispettare e, dunque, a garantire tale diritto che, in forza dell'art 51, Carta dei diritti fondamentali dell'Unione Europea, vale anche per gli Stati membri nell'attuazione del diritto dell'Unione[11].
La stessa Corte EDU, da tempo, invero, e, più precisamente, in epoca assai più risalente rispetto ai Giudici di Lussemburgo, ha ricondotto l'acquisizione e la conservazione di questi dati *sub* art. 8 CEDU[12], disposto che tutela non solo il diritto all'identità e allo sviluppo della personalità, ma altresì quello di stabilire e sviluppare relazioni umane, su cui incidono negativamente la raccolta e conservazione sistematica di dati. In queste ipotesi[13], i Giudici di Stra-

---

dati personali verso gli Stati Uniti. Evoluzioni e prospettive di diritto comparato, in *Responsabilità e tutela dei diritti*, Napoli, 2018, 4. Per una ulteriore disamina, in argomento v. altresì PITTIRUTI, *Digital evidence e procedimento penale*, Torino, 2017, *passim* nonché SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa,* Torino, 2018, passim.

[8] Testualmente art. 8 Carta dei diritti fondamentali UE: «Protezione dei dati di carattere personale 1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

[9] Così art. 7, Carta dei diritti fondamentali dell'Unione europea «Rispetto della vita privata e della vita familiare. Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni».

[10] Cfr. articolo 16 (*ex* articolo 286 del TCE), Trattato sul funzionamento dell'Unione europea, testualmente: «1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti. Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea».

[11] Per una approfondita disamina della normativa di riferimento sia concesso il rinvio a TEROLLI, *Privacy e protezione dei dati personali UE vv USA. Evoluzione di diritto comparato e il trasferimento dei dati dopo la sentenza "SCHREMS II",* in *Diritto dell'Informazione e dell'Informatica (II),* 2021, 1, 49.

[12] La Carta UE si differenzia allora dalla CEDU, la quale tutela invece la protezione dei dati come parte del più ampio diritto al rispetto della vita privata e familiare (articolo 8 Cedu).

[13] Cfr. Corte EDU, Uzun v. Germany, 2 settembre 2010, ric. n. 35623/05; Corte EDU, 4 maggio 2000, Rotaru v. Romania, ric. n. 28341/95; Corte EDU, 2 agosto 1984, Malone v. United Kingdom, ric. n. 8691/79

sburgo hanno avuto modo di raccomandare un bilanciamento tra gli interessi contrapposti al fine di accertare, con riferimento a tutte le circostanze di ciascuna fattispecie, se è stato osservato o meno un giusto equilibrio tra tali interessi ed escludendo recisamente la costruzione di una aprioristica gerarchia all'interno di questi diritti, tutti, peraltro, *species* del più ampio *genus* delle libertà fondamentali dell'individuo.

Parzialmente diverso l'approccio delle Corti costituzionali nazionali che, essenzialmente, sono solite ricondurre l'attività in questione al diritto alla libertà e segretezza delle comunicazioni. Con specifico riferimento alla situazione italiana, precedentemente all'introduzione del c.d. Codice *privacy* si era acceso un frenetico dibattito –sorto per individuare la copertura costituzionale di una attività, all'epoca, priva di disciplina legislativa- relativo alla riconducibilità dell'attività di conservazione e acquisizione dei dati di traffico *sub* art. 15 o *sub* art. 2 Cost. risolto, invero, dal Giudice delle Leggi con una pronuncia che esalta(va) l'ampiezza della tutela accordata dall'art. 15 Cost. «*è sicuramente tale da ricomprendere fra i propri oggetti anche i dati esteriori di individuazione di una determinata conversazione telefonica*»[14]. Infatti, la Costituzione tutela non solo la segretezza, ma anche la libertà delle comunicazioni, offrendo così una protezione molto ampia al diritto dei singoli di intrattenere relazioni riservate. I termini del dibattito devono tuttavia ritenersi oramai ampiamente superati alla luce del rinnovato contesto interno e sovranazionale[15].

In ogni caso, la tutela della protezione dei dati nella UE non è lasciata alla sola azione di controllo della Corte di giustizia, influenzata quest'ultima –non può sottacersi- inevitabilmente, tanto dagli orientamenti espressi nelle precedenti pronunce rese in materia dagli stessi Giudici, tanto da quelle dei Tribunali nazionali in merito alle problematiche di compatibilità con il diritto alla *privacy* e il diritto alla protezione dei dati personali sollevate dal regime istituito dalla direttiva sulla *data retention*.

Invero, lo stesso legislatore europeo, gradatamente, ha costruito un quadro normativo di protezione, completo ed adeguato –il più possibile– alle nuove esigenze del sistema internazionale[16].

---

[14] Così: Corte cost., n. 81 del 1993. Conforme, Id., n. 281 del 1998. In dottrina, si veda, *ex multis,* CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Riv. it. dir. e proc. pen.,* 2005, 594 ss. nonché ampiamente CAPRIOLI, *Colloqui riservati e prova penale*, Torino, 2000, *passim*. V. altresì in argomento COMELLA, *Alcune considerazioni sugli aspetti tecnologici della sorveglianza di massa, a margine della sentenza "Safe Harbor" della Corte di giustizia dell'Unione europea,* in *Dir. informaz. e informatica*, 2015, 4-5, 719.

[15] Cfr. *infra*.

[16] Per un quadro dettagliato della normativa di riferimento v. CRESPI, *Rivista*, cit., .3-4, 2015, 819.

In particolare, la normativa sul trattamento dei dati personali -che già figura(va) *sub* articolo 16 TFUE e che pure pone(va) in capo al legislatore europeo la competenza concorrente con gli Stati membri ad adottare, secondo la procedura ordinaria, le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché quelle connesse alla libera circolazione di tali dati[17]– è, oggi, disciplinata in modo unitario dal Regolamento 2016/679, meglio noto con l'acronimo GDPR (*General data protection regulation*)[18] emanato al fine precipuo di garantire maggiore riservatezza e trasparenza negli accordi di *privacy policy* con gli utenti[19]. *Ivi* è enucleata espressamente la definizione di dato personale che ricomprende, una miriade di tipi di dati come: il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online, informazioni sul conto bancario o carta di credito, le cartelle cliniche, informazioni sul passaporto, indirizzo e-mail personale, foto e video, nome utente e *password* ecc.[20]

Ulteriore strumento normativo previsto nell'ordinamento europeo che, unitamente al GDPR istituisce un quadro giuridico per garantire la *privacy* digitale a tutti i cittadini dell'Unione europea è il Regolamento ePrivacy che, sinteticamente, per quel che rileva nel presente lavoro- prevede norme

[17] Cfr. *amplius* CORTESE, *La protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona*, in *Dir. Un. eur.,* 2013, 2, 43.

[18] Operativo dal 25 maggio 2018, data di entrata in vigore del GDPR, ha abrogato la Direttiva 95/46/CE e, di fatto, unificato un *patchwork* di 28 diverse leggi sulla *privacy* degli Stati membri, determinando, pertanto un passaggio cruciale e ambizioso in materia di protezione dei dati personali. Si compone di 173 Considerando, ai quali seguono 99 articoli, suddivisi in 11 capi. Dalla disamina dei Considerando del Regolamento stesso si evince come, per espressa previsione il trattamento dei dati personali debba essere «al servizio dell'uomo»; conseguentemente il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. In argomento, cfr. DURST, *Il Regolamento Europeo per la protezione dei dati personali tra privacy e trasparenza*, in Arco di Giano, 2021, 107, 47 ss.

[19] Gli accordi di *privacy policy* sono quelli che interccorrono tra le aziende che forniscono l'accesso ai servizi telematici e telefonici -cd. Internet Service Providers (Isp)- e gli utenti "finali" e sono finalizzati a consentire, a questi ultimi, l'accesso alla rete telefonica e telematica identificata attraverso un numero di telefonia e un precipuo indirizzo IP fornito dallo stesso ISP. Sul punto sia concesso il rinvio a GIANGRECO, *Data retention, acquisizone e utilizzabilità dei tabulati telefonici e telematici: una riflessione incrociata - Data retention, acquisition and usability of phone and telematic records: a cross-cutting reading* in *Cass. pen.,* 2022, 4, 1673.

[20] Cfr. art 4. GDPR: «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

aggiuntive sulla protezione dei dati per reti di telecomunicazione e servizi Internet. ePR tese a proteggere la riservatezza delle comunicazioni, i dati personali e non, i contenuti ed i metadati (fonte, destinazione, posizione del dispositivo, data, ora, durata)[21].

Nel Regolamento non è però delineato alcun limite temporale per la conservazione dei suddetti[22] e neppure si ritiene sia applicabile ai trattamenti dei dati personali effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali; neppure trova applicazione in alcuni altri casi, invero, disciplinati nella Direttiva 2016/680/UE attuata, con decreto legislativo n. 51 del 18 maggio 2018.

Di rilievo in materia, è altresì, la normativa rivolta agli *Internet Service Providers*, relativa ai tempi di *data retention* per finalità penali di cui all'art. 132 del d.lg. 196/2003 (c.d. codice privacy), in combinato disposto con l'art. 24 della l. 167/2017 (c.d. legge europea 2017)[23]che differenzia, «*con un doppio binario, l'obbligo di conservazione dei metadati in relazione al tipo di reato e al tipo di dato richiesto*»[24] per cui, precisamente: per i reati c.d. comuni, i dati telefonici devono essere conservati per 12 mesi dalla loro registrazione, i dati telematici per 24 mesi e le chiamate senza risposta per 30 giorni; diversamente, per i reati c.d. speciali di cui agli artt. 51, comma 3-quater, c.p.p. e 407, comma 2, lettera a) c.p.p., invece, tutti i dati, telefonici e telematici, sono acquisibili entro 72 mesi dal momento della loro creazione[25].

---

[21] Trattasi, precisamente, di *Lex specialis* al GDPR. Il Regolamento ePrivacy e il GDPR sono andati di pari passo così come la Direttiva ePrivacy e la Direttiva 95/46/EC. In particolare, si evidenzia come la Direttiva ePrivacy è la 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 (direttiva relativa alla vita privata e alle comunicazioni elettroniche).

[22] Tentativi di colmare siffatta lacuna sono stati posti in essere dal Garante per la protezione dei dati personali: Cfr. Garante per la protezione dei dati personali, *GDDP, 'Fidelity card' e garanzie per i consumatori. Le regole del Garante per i programmi di fidelizzazione*, in *www.garanteprivacy.it*, secondo cui: «*i dati relativi al dettaglio degli acquisti con riferimento a clienti individuabili possono essere conservati per finalità di profilazione o di marketing per un periodo non superiore, rispettivamente, a dodici e a ventiquattro mesi dalla loro registrazione*».

[23] L. 20 novembre 2017, n. 167 a cui rinvia il comma 5 *bis* dell'art. 132 Codice privacy. In particolare, suddetta legge è stata approvata, come si legge nel suo art. 24 comma 1, «in attuazione dell'articolo 20 della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio».

[24] Così GIANGRECO, *Data retention, acquisizione e utilizzabilità dei tabulati telefonici e telematici: una riflessione incrociata*, cit., 1675. In argomento v. altresì DI STEFANO, *La corte di giustizia interviene sull'accesso ai dati di traffico telefonico e telematico e ai dati di ubicazione a fini di prova nel processo penale*, in *Cass. pen.*, 2021, 7-8, 2563.

[25] Cfr. ancora in argomento, GIANGRECO, *Data retention, acquisizone e utilizzabilità dei tabulati telefonici e telematici: una riflessione incrociata*, cit., 1672.

L'articolo 15, paragrafo 1, della direttiva 2002/58 CE relativa alla vita privata e alle comunicazioni elettroniche[26], inoltre, ai sensi dell'articolo 5, paragrafo 1, impone agli Stati membri di garantire, mediante la propria legislazione nazionale, la riservatezza delle comunicazioni effettuate tramite una rete pubblica di comunicazione e di servizi di comunicazione elettronica accessibili al pubblico, nonché la riservatezza dei relativi dati sul traffico.
Consegue che gli Stati membri hanno l'obbligo di vietare alle persone diverse dagli utenti di ascoltare, captare, memorizzare le comunicazioni e i relativi dati sul traffico o di sottoporle a qualsiasi altro mezzo di intercettazione o di sorveglianza, senza il consenso degli utenti interessati, salvo quando tale persona vi sia legalmente autorizzata, conformemente all'articolo 15, paragrafo 1, della medesima direttiva.
La conservazione dei dati relativi al traffico e dei dati relativi alla ubicazione quindi costituisce, di per sé, da un lato, una deroga al divieto, previsto dall'articolo 5, paragrafo 1, della direttiva 2002/58, per qualsiasi persona diversa dagli utenti di memorizzare tali dati e, dall'altro, un'ingerenza nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali, sanciti dagli articoli 7 e 8 della Carta, a prescindere dalla circostanza che le informazioni relative alla vita privata di cui trattasi abbiano o meno un carattere sensibile, che gli interessati abbiano o meno subito eventuali inconvenienti in seguito a siffatta ingerenza, o che i dati conservati siano o meno utilizzati successivamente.
In questo contesto, dalla formulazione stessa dell'articolo 15, paragrafo 1, della direttiva 2002/58 discende che gli Stati membri possano adottare una misura che deroghi al principio di riservatezza soltanto ove tale misura sia «necessaria, opportuna e proporzionata all'interno di una società democratica», alla luce degli obiettivi enunciati, nonché «strettamente» proporzionata allo scopo perseguito.
La tutela del diritto fondamentale al rispetto della vita privata esige che eventuali deroghe e restrizioni alla tutela dei dati personali operino entro i limiti

[26] La suddetta direttiva ha lo scopo, come risulta in particolare dai considerando 6 e 7, di tutelare gli utenti dei servizi di comunicazione elettronica, dai pericoli per i loro dati personali e la loro vita privata derivanti dalle nuove tecnologie e, in particolare, dalla maggiore capacità di memorizzazione e di trattamento automatizzati di dati. Come enunciato dal considerando 2 della medesima direttiva, la volontà del legislatore dell'Unione è di garantire il pieno rispetto dei diritti di cui agli articoli 7 e 8 della Carta (v., in tal senso, le sentenze rese dai Giudici di Lussemburgo: del 21 dicembre 2016, Tele2 Sverige e Watson e a., C-203/15 e C-698/15 nonchè del 6 ottobre 2020, La Quadrature du Net e A., C-511/18, C-512/18 e C-520/18, EU).

dello stretto necessario[27].

3. *L'esegesi dei Giudici UE.* L'assenza di regole europee dettagliate e tese ad individuare, in maniera stringente, come autorevolmente rilevato «affidabili categorie di bilanciamento tra i diritti di *privacy* e altri diritti»[28], ha inevitabilmente indotto la Corte di giustizia, come accennato nell'epigrafe del presente lavoro, a porre rimedio a questa vacuità normativa, enucleando una serie di principi –sempre in tema di *data retention*- da valere quale griglia di *standards* minimi per consentire il giudizio di bilanciamento tra il diritto alla riservatezza e quello di prevenzione dei reati.

La recente sentenza resa dai Giudici di Lussemburgo in data 5 aprile 2022, si inserisce, precipuamente, in un contesto di particolare sensibilità a livello europeo per il tema del rapporto tra tecnologia informatica e diritti fondamentali della persona, nel solco già tracciato dalle pronunce emanate in argomento, dagli stessi giudici -sin dal 2014- tese, tutte, a circoscrivere le attività di acquisizione con riferimento a procedimenti penali aventi ad oggetto forme gravi di criminalità e di garantire che dette attività siano soggette al controllo di un'autorità giurisdizionale.

La attenta disamina del contenuto della recentissima pronuncia sembra invero fare eco a quanto già dalla stessa Corte di giustizia UE evidenziato nelle note pronunce *Digital Rights*[29] e *Tele2*[30], nelle quali i giudici europei avevano già ampiamente segnalato come la conservazione dei dati esterni alle comunicazioni comportasse un'ingerenza nel diritto alla riservatezza ed alla tutela della vita privata dei singoli utenti, con la conseguenza che gli ordinamenti nazionali sono stati già da tempo chiamati a predisporre una normativa che individuasse specifici limiti di carattere sia "statico" che "dinamico".

La odierna pronuncia di aprile 2022 ha ribadito con ancor più forza come il diritto dell'Unione è contrario a misure legislative che prevedono una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione afferenti alle comunicazioni elettroniche, anche qualora l'esigenza sottesa sia quella della finalità di lotta ai reati gravi.

Difatti, quest'ultimo obiettivo, per quanto fondamentale, non può, di per sé,

---

[27] Cfr., in tal senso, Corte giust. UE, 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, punti 115 e 116, e giurisprudenza citata.

[28] Così VALENTINI, *Forme di privazione del diritto di difesa nello Stato senza diritto (ovvero: come un gioco di parole diventa realtà),* cit., *passim*.

[29] Corte Giust. UE, 8 aprile 2014, Digital Rights Ireland, cause riunite C-293/12 e C-594/12.

[30] Corte Giust. UE, 21 dicembre 2016, Tele 2 e Watson, cause riunite C-203/15 e C-698/15.

solo, giustificare una misura di conservazione generalizzata ed indifferenziata dei dati relativi al traffico e di quelli relativi all'ubicazione; il principio generale di tutela della riservatezza dell'individuo non può essere *sic et simpliciter* derogato nemmeno in casi di perseguimento di reati gravi o gravissimi ma presuppone, sempre e comunque, il rispetto dei requisiti di idoneità e di necessità, e quello relativo al carattere proporzionato di tali misure in relazione all'obiettivo perseguito.

Con riferimento a quest'ultimo criterio, inoltre, la enunciazione del conseguimento di un obiettivo di interesse generale deve essere conciliato con i diritti fondamentali interessati dalla misura, effettuando un contemperamento equilibrato tra, da un lato, l'obiettivo di interesse generale e, dall'altro, i diritti di cui trattasi[31].

I medesimi moniti, invero, erano già stati espressi -sempre dalla Corte di giustizia- nella notissima pronuncia H.K.[32] nella quale, ancor più vigorosamente, è(ra) già stato sottolineato come l'art. 15 della direttiva 2002/58/CE consenta una limitazione dei diritti sanciti agli artt. 7 e 8 Carta dei Diritti Fondamentali dell'Unione Europea solo a seguito di una stringente valutazione di necessità, opportunità e proporzionalità avuto riguardo alla repressione delle sole « forme gravi di criminalità ».

Il pregio della sentenza da ultimo citata, invero, si ricorderà, è stato quello di scuotere la mente del legislatore italiano ad un totale *revirement* dell'art. 132 Codice *privacy*, imponendo cioè «*in un colpo solo la giurisdizionalizzazione del procedimento di acquisizione dei tabulati e la subordinazione* dell'acquisizione all'esigenza di accertare gravi reati[33]» attraverso l'emanazione, d'urgenza, del d.l. 30 settembre, n. 132 [34].

Nella pronuncia della Corte di giustizia testé richiamata, dello scorso anno, era stata espressa una ulteriore interpretazione non dissimile a quella pure

---

[31] Così già Corte Giust. UE, 6 ottobre 2020, La Quadrature du Net e a., C-511/18, C-512/18 e C-520/18, EU:C:2020:791. In particolare v. punto 130.

[32] Corte giust. UE, 2 marzo 2021, H.K., C-746/18.

[33] Così GIANGRECO, *Data retention, acquisizione e utilizzabilità dei tabulati telefonici e telematici: una riflessione incorciata,* in *Cass. pen.*, 2022, 1676.

[34] D.l. 30 settembre 2021, n. 132 (conv. L. 23 novembre 2021, n. 178). Alla base del suddetto intervento del legislatore vi era l'esigenza di adeguare la normativa sulla *data retention* ai «principi enunciati dalla Grande sezione della Corte di giustizia dell'Unione europea nella sentenza del 2 marzo 2021, causa C-746/18, e in particolare di circoscrivere le attività di acquisizione ai procedimenti penali aventi ad oggetto forme gravi di criminalità e di garantire che dette attività siano soggette al controllo di un'autorità giurisdizionale». Cfr. *Dossier Camera dei deputati: Misure urgenti in materia di giustizia e di difesa, nonché proroghe in tema di referendum, assegno temporaneo e IRAP. Elementi per l'esame in Assemblea*, in *www.temi.camera.it,* 2021, 6.

ribadita nella pronuncia del 5 aprile 2022, oggetto di disamina: difatti, (già) in quell'occasione, la Corte aveva individuato *sub* art. 15 della Direttiva UE 58/2002 un ostacolo all'introduzione di misure di prevenzione, accertamento e perseguimento dei reati che consentissero l'utilizzo dei dati in oggetto senza alcuna limitazione connessa alla durata, alla quantità e alla natura dei dati trattati, e al di fuori del perimetro della repressione di forme gravi di criminalità e/o della tutela della pubblica sicurezza, senza purtuttavia chiarire le condizioni specifiche che rendono l'utilizzo dei dati di traffico e di localizzazione, anche per fini preventivi degli illeciti, conforme alla disciplina europea.
L'odierna pronuncia invero, si spinge "ancor più in là" rispetto alla interpretazione resa un anno prima, poiché procede ad individuare accuratamente, sulla base di una rigorosa valutazione in termini di proporzionalità, le condizioni per consentire la "compromissione" al diritto al rispetto alla vita privata e di quello alla tutela dei dati personali cui la stessa dà vita.
Sinteticamente, ad avviso dei Giudici di Lussembrugo si rende assolutamente necessario individuare precisi limiti alla conservazione, circoscrivendola, ad esempio, ad un particolare periodo o ad una zona geografica o ad una cerchia di persone che potrebbero essere coinvolte in crimini gravi.
Ciò, evidentemente, al fine di evitare una conservazione indiscriminata dei dati di tutte le comunicazioni di tutte le persone, senza alcuna differenziazione di sorta.
La recente pronuncia di aprile 2022, reca comunque un *quid pluris* di "innovativo" rispetto a quanto già sancito dai giudici di Lussemburgo, nella parte in cui la Corte esprime –quasi con un giudizio prognostico *ex ante*– la conformità ai dettami europei di quelle disposizioni –evidentemente nazionali– volte ad introdurre, per le finalità di prevenzione di illeciti e tutela della sicurezza pubblica, misure che rechino determinati limiti intrinseci per ciascuna categoria di dato e, precisamente: la conservazione mirata dei dati relativi al traffico e dei dati relativi all'ubicazione (a condizione che questa sia delimitata, si basi su elementi oggettivi e non discriminatori, in funzione delle categorie di persone interessate o mediante un criterio geografico, per un periodo temporalmente limitato allo stretto necessario, ma rinnovabile); la conservazione generalizzata e indifferenziata degli indirizzi IP attribuiti all'origine di una connessione, per un periodo temporalmente limitato allo stretto necessario; la conservazione generalizzata e indifferenziata dei dati relativi all'identità civile degli utenti di mezzi di comunicazione elettronica; il ricorso ad un'ingiunzione rivolta ai fornitori di servizi di comunicazione elettronica, mediante una decisione dell'autorità competente soggetta ad un controllo giuri-

sdizionale effettivo, di procedere, per un periodo determinato, alla conservazione rapida dei dati relativi al traffico e dei dati relativi all'ubicazione di cui dispongono tali fornitori di servizi.

4. *La disciplina in vigore in Italia: punti di attrito con la giurisprudenza dei Giudici UE.* Già si è accennato al fatto che, sulla scia dei moniti sanciti dai Giudici di Lussemburgo, l'Italia abbia provveduto urgentemente –come *infra* anticipato– a novellare, oramai lo scorso anno, l'articolo 132 del Codice Privacy, emendando il comma 3 ed introducendo i commi 3 *bis*, 3 *ter* e 3 *quater*.

L'attuale disciplina prevede che il pubblico ministero e le altre parti legittimate *ex lege* (quali: difensore, imputato, indagato, persona offesa e altre parti private) possano presentare «*un'istanza*» al giudice per richiedere l'emissione di un decreto motivato che autorizzi l'acquisizione dei dati conservati presso i gestori «*entro il termine di conservazione imposto dalla legge*» qualora sussistano sufficienti indizi di reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, e di reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi[35].

In ordine a questa procedura "ordinaria", il legislatore italiano non ha, però, delineato alcuna indicazione in ordine alla concreta metodologia acquisitiva seguente all'emissione del decreto motivato di autorizzazione e, men che mai, ha provveduto ad enucleare le modalità per consentire che l'acquisizione richiesta da una parte e da costei ottenuta, sia poi "controllabile" dall'altra, non soltanto al fine di conoscere concretamente, nel merito, il relativo contenuto acquisito ma anche per valutare la correttezza dell'*iter* seguito per la relativa "apprensione", saggiandone la affidabilità.

La considerazione, sia permesso rilevare, non è di poco conto poiché è strettamente correlata al diritto di difesa inteso nella sua accezione dinamica: il difensore deve, infatti, poter materialmente prendere visione e, correlativamente, estrarre copia -senza se e senza ma- di tutto quanto necessario alla difesa del suo assistito.

Inoltre, proprio questa ulteriore considerazione riecheggia recenti e più autorevoli valutazioni, seppur queste svolte con riferimento alla disciplina delle intercettazioni, sotto il profilo dell'inaccettabile annichilimento, in determinate situazioni, del diritto di difesa e del correlativo diritto alla ricerca della pro-

[35] Sulla gravità dei reati presupposto, la sufficienza indiziaria e la rilevanza per l'accertamento dei fatti v. ampiamente GIANGRECO, *Data retention, acquisizione e utilizzabilità dei tabulati telefonici,* cit., 1676.

va[36].

Quanto invece ai casi di particolare urgenza ed al fine di evitare pregiudizio per le indagini[37], il disposto normativo così come novellato consente l'acquisizione dei dati con decreto motivato del pubblico ministero, comunicato immediatamente, ed al più entro 48 ore, al giudice competente per la convalida entro le successive 48 ore.

Nulla si rinviene, nel disposto normativo *de quo,* in ordine alle conseguenze che si profilano nel caso di mancata convalida, da parte del giudice, ai sensi del comma 3 *quater* dell'art. 132 Codice *Privacy*; una previsione espressa sul punto, che non lasciasse spazio ad eventuali "ripresentazioni" di istanze tese a sanare l'acquisizione di dati già non convalidati sarebbe stata, invero, tanto più opportuna considerato che una prassi distorta, di questo tenore, potrebbe addirittura rendere utilizzabili dati non più acquisibili per decorso dei termini di *data retention*.

La disciplina in vigore, nonostante lo sforzo di adeguarsi alla esegesi europea, purtuttavia, non pare conforme agli orientamenti della Corte di giustizia, soprattutto con riferimento ai moniti da ultimo espressi nella recente pronuncia del 5 aprile.

In primo luogo, la pur recente riforma italiana, non ha minimamente intaccato la possibilità per il fornitore di conservare -anche fino a anni sei, per finalità di accertamento e repressione dei reati, dati di traffico telefonico e telematico, nonché dati relativi alle chiamate senza risposta, anche fino a sei anni dalla comunicazione, così come previsto dalla richiamata Legge 167/2017 (Legge Europea 2017), *sub* art. 24.

Questo amplissimo arco temporale di conservazione, non soltanto pare stridere –come peraltro espressamente dichiarato dallo stesso Garante–[38] con la (fortissima) cultura formatasi, tanto in Europa quanto in Italia, in tema di protezione dei dati l'indomani dall'entrata in vigore del GDPR, ma soprattutto, non può sottacersi come la previsione, in ogni caso, cozzi con l'architettura

---

[36] Così per una attenta ad autorevole riflessione in argomento, v. ampiamente VALENTINI, *Forme di privazione del diritto di difesa nello Stato senza diritto (ovvero: come un gioco di parole diventa realtà*), cit., *passim*.

[37] Cfr. comma 3 *bis* dell"art. 132 Codice *privacy*.

[38] L'Autorità in queatione ha anche recentemente rimarcato la necessità di ridurre i termini di conservazione dei dati in oggetto «*riconducendoli entro margini maggiormente compatibili con il canone di proporzionalità, tenendo conto dei precedenti sui quali la Corte di giustizia dell'Unione europea ha avuto modo di pronunciarsi*». Cfr. "*Parere sullo schema di decreto-legge per la riforma della disciplina dell'acquisizione dei dati relativi al traffico telefonico e telematico a fini di indagine penale*" del 10 settembre 2021 reperibile on line sul sito *www. Parere sullo schema di decreto-legge per la riforma della disciplina... - Garante Privacy (gpdp.it)*

garantista che (dovrebbe) sorregge(re) il rito penale.
L'eccessiva estensione temporale della conservazione dati deve infatti essere necessariamente rivisitata non potendo tollerarsi, in uno stato democratico, un "diritto", così dilatato, al controllo sul flusso di informazioni della persona.
Paradossale, sotto questo profilo, ulteriormente considerare come molto spesso la stessa persona che subisce siffatta ingerenza non abbia poi alcun contrappeso da far valere, in termini di controllo, sull'uso medesimo di questi (suoi) dati.
Ma non è soltanto un problema di tempi di conservazione "da accorciare": l'articolo 132 del Codice *Privacy*, non prevede alcuna differenziazione delle modalità di trattamento a seconda della categoria in cui rientrano i dati oggetto di indagine diversamente da quanto invero ribadito dai Giudici di Lussembrugo nella recente pronununcia dell'aprile 2022, nella quale sono stati delineati veri e propri differenti livelli di garanzia per l'interessato, a seconda che oggetto di trattamento siano, per esempio, dati relativi al traffico o all'ubicazione– per i quali è ammessa esclusivamente la conservazione mirata e limitata alla sussistenza di elementi oggettivi e non discriminatori –oppure l'indirizzo IP, che –si ritiene–possa essere oggetto finanche di conservazione generalizzata e indifferenziata.
La normativa attuale interna, conseguentemente, non è –ad avviso di chi scrive– in grado di offrire adeguata protezione ai diritti, tutti, oggetto di tutela e, comunque, dimostra concretamente la sua inadeguateza ad adattarsi ai cambiamenti imposti tanto dall'ordinamento sovranazionale tanto dall'esegesi dei giudici europei.

5. *Qualche conclusione.* Secondo uno studio condotto nel 2017, gli strumenti di indagine più utilizzati in Europa sono, oltre le captazioni preventive, proprio i sistemi di sorveglianza di massa[39].
In questo modo, gli investigatori diventano protagonisti indiscussi della ricerca di una verità diversamente concepita, tesa *in primis*, alla raccolta ed all'analisi delle notizie apprese attraverso l'attività di sorveglianza sulle comunicazioni e sugli scambi di dati tra gli individui per poi confluire nell'elaborazione di strategie di anticipazione e neutralizzazione dell'offesa[40].

[39] Cfr. *European Union Agency for Fundamental Rights, Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU: Mapping Member States' legal frameworks*, October 2017, disponibile al sito *www.fra.europa.eu*

[40] Per approfondimenti relativi ad ulteriori attività atipiche svolte, sempre nella fase pre-investigativa, dalla polizia giudiziaria, sia concesso il rinvio a CECANESE, *Le pre-investigazioni informatiche e i controlli sui social*, in *Pre-investigazioni (Espedienti e mezzi)*, a cura di Scalfati, cit., 267 ss. nonché: LOPEZ,

Sotto questo profilo, pare effettivamente anacronistico ritenere che il procedimento penale si instaura con l'acquisizione della *notitia criminis*[41]; pur non sottacendo che, tradizionalmente, l'inizio dell'*iter* procedimentale sia effettivamente (ancora) determinato dall'iscrizione della notizia di reato nell'apposito registro, non è possibile comunque, oggi, non riscontrare la esistenza di una precisa attività preventiva e di ricerca della *notitia criminis* medesima che, inevitabilmente, indirizza le investigazioni "per" procedere alla sua formazione[42].

In altre parole, l'attività "*preventiva*" procedimentale (o come definita nella letteratura scientifica, da taluni, "indagine proattive") spinge per una circolazione probatoria di dati ed informazioni e per un'implementazione di essi, eventualmente raccolti, nella fase delle indagini.

Ciò unitamente alla nuova cultura della prevenzione, improntata all'anticipazione della risposta penale rispetto alla consumazione del fatto di reato, determina in modo inesorabile il progressivo spostamento dell'«*asse strategico dell'indagine [...] verso modalità occulte di provvista di informazioni*»[43], finendo così per esaltare il ricorso all'azione di sorveglianza sulle comunicazioni e sugli scambi di dati tra gli individui quale rimedio privilegiato per prevenire la minaccia terroristica[44] o comunque, un reato di grave allarme so-

---

I*ndividuazione facciale tramite software e individuazione del sospettato*, *ivi*, 295 ss.; TROISI, *Dati P.N.R. e trattamento pre-investigativo, ivi,* 319 ss. Invece, relativamente agli atti tipici posti in essere dalla polizia giudiziaria cfr. TRIGGIANI, *Indagini preliminari*, in *Manuale di Diritto processuale penale*, 3a ed., a cura di Scalfati, Bernasconi, De Caro, Furgiuele, Menna, Pansini, Triggiani, Valentini, Torino, 2018, 463 ss.

[41] La considerazione *de qua* muove dalla attenta ed autorevole disamina di GIUNCHEDI, *Le attività di prevenzione e i ricerca di intelligence*, in *La prova penale*, a cura di GAITO, 2008, II, 1.

[42] Ancora, in argomento, sia concesso il rinvio a NOCERINO, *Le intercettazioni e i controlli preventivi sulle comunicazioni. Strumenti d'indagine a rischio di "infiltrazioni processuali"*, in *Riv. it. dir. e proc. pen., 2*019, 2, 881.

[43] In questi termini NEGRI, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico)*, in *Arch. pen.*, 2016, 2, 43. V. altresì esaustivamente in argomento, SPANGHER, *Considerazioni sul processo "criminale" italiano,* Torino, 2015, 7 ss.

[44] Così GIUNCHEDI, *Le attività di prevenzione e di ricerca di intelligence*, cit., 1. In argomento v. altresì ANDOLINA, *Le intercettazioni e i controlli preventivi sulle comunicazioni nel contrasto al terrorismo internazionale tra irrisolte criticità ed esigenze di riforma*, in *Arch. nuova proc. pen.,* 2016, 6, 568 nonché MILITELLO, *Terrorismo e sistema penale: realtà prospettive e limiti*, in *Dir. pen. cont.*, 2017, 1, 5. Per ulteriori autorevoli considerazioni sempre relative all'argomento oggetto del presente lavoro, non può non richiamarsi altresì l'espressione utilizzata da GIOSTRA, *Il processo penale «contro» la criminalità organizzata: rischi di strumentalizzazione*, in *Lotta alla criminalità organizzata: strumenti normativi*, a cura di Giostra - Insolera, Milano, 1995, 155, il quale ha osservato molto efficacemente come: « (...) *quando si afferma che il processo è un'arma contro il crimine, siamo in presenza, come diceva Borghese a proposito dei versi di D'Annunzio, di una giacca abbottonata non in giusta aderenza con le asole. Altri sono gli strumenti di lotta alla criminalità* (...)».

ciale.
In questo quadro, gli equilibri di potere tra i protagonisti delle tradizionali indagini preliminari risultano alterati, ingenerando una confusione di ruoli assai "pericolosa"[45]: sono gli investigatori (e più precisamente, sia le Forze di polizia che Servizi d'*intelligence*) a "guidare" le investigazioni e ad orientare il procedimento penale detenendo, peraltro, il monopolio strategico della mole di informazioni raccolte in autonomia e con largo anticipo rispetto all'intervento dell'autorità giudiziaria[46].
Ma il punto è che il ricorso a queste forme di controllo quale tecnica privilegiata per neutralizzare i fenomeni di grave allarme sociale ed assicurare la protezione della sicurezza collettiva, determina evidentemente innumerevoli punti di frizione con l'ordinamento costituito, entrando in conflitto non solo con le regole processuali[47] scandite nell'attuale codice di rito, *strictu sensu* intese, ma anche con i valori che fondano –o che meglio dovrebbero fondare- il sistema e, più in generale, l'essenza di uno Stato democratico: ciò non solo in ragione dei risvolti processuali che questo tipo di attività inevitabilmente causa, ma anche alla luce della permanente compromissione agli spazi di libertà individuale, peraltro non giustificata dalla sola commissione di un fatto di reato e men che mai dalla presunta colpevolezza del soggetto "monitorato".
Neppure può sottacersi, sotto altro profilo, come anche con riferimento alla *data retention*, sia riscontrabile una scarsa sensibilità dei giudici nel riconoscerne eventuali profili di invalidità; più precisamente, secondo un percorso

[45] Sia nella fase delle indagini sia in quella ancor precedente delle pre-indagini, il pubblico ministero è sostanzialmente "solo" senza confronto con la difesa. Sugli ampi spazi di discrezionalità che connoterebbero le scelte del pubblico ministero in queste due fasi v. BRUTI LIBERATI, *Le scelte del pubblico ministero: obbligatorietà dell'azione penale, strategie di indagine e deontologia,* in *Quest. giust.,* 2018, 1, 14 e ss. nonché VALENTINI, *La completezza delle indagini, tra obbligo costituzionale e (costanti) elusioni della prassi*, in questa rivista, 2019, reperibile in *questa Rivista.*

[46] Per un'ampia trattazione della problematica v. NOCERINO, *Le intercettazioni e i controlli preventivi sulle comunicazioni,* cit., 881. Diffusamente, v. altresì CURTOTTI *Procedimento penale e intelligence in Italia: un'osmosi inevitabile, ancora orfana di regole*, in *Proc. pen. giust.*, 2018, 3, 438 nonché TRIGGIANI, S*ervizi di "intelligence", segreto di Stato e intercettazioni preventive: appunti sulla "riforma della riforma",* in *Legislaz. pen.,* 2013, II, 285 ss.

[47] Sula crisi della legalità nella fase investigativa, a partire dalla ricerca della notizia di reato ad opera del pubblico ministero sino all'iscrizione tardiva della *notitia criminis* nel registro, dalle indagini atipiche alle investigazioni *undercover* v. ampiamente TRIGGIANI, *Legalità opaca: raccolta atipica e pre-investigazioni,* in questa rivista, 2021, 1, reperibile anche *on line* in *questa Rivista*- Ad avviso dell'ill.stre A. emergono vere e proprie zone d'ombra, nelle quali gli organi inquirenti si muovono senza sottostare ad alcuna forma di controllo giurisdizionale, con evidente compromissione del diritto di difesa dell'indagato e, più in generale, dei diritti fondamentali della persona.

comune anche ai campi della *scientific evidence*, molto spesso il libero convincimento dell'organo *decidendi* diventa il viatico per legittimare un approccio antiformalistico in tema di acquisizione della prova[48].

Ebbene, tale ricostruzione va senz'altro contrastata poiché la unica risposta possibile ad un (qualsivoglia) elemento probatorio formatosi senza il necessario rispetto dell'integrità dello stesso ed in spregio alla metodologia acquistitiva delineata per la sua apprensione, deve, senza dubbio, essere la declaratoria di inutilizzabilità probatoria ai sensi dell'art. 191 c.p.p.[49]

Non deve essere possibile, né può essere in alcun modo accettato, "compensare" le violazioni relative alle modalità di formazione perché queste incidono necessariamente sulla prova stessa fino a rendere del tutto inattendibile l'accertamento frutto di tali risultanze[50].

Sulla base di queste premesse, l'obiettivo prioritario da perseguire, anche al fine di evitare un vero e proprio *blak out* del sistema delineato nell'attuale codice di rito penale, *in primis* da parte degli studiosi del rito penale, ma dovrebbe esserlo anche per lo stesso legislatore nazionale, è quello di rincanalare negli argini delle regole, le deviazioni cui assiste, tenendo ben a mente che la contingenza impone un riordino e un rinnovo delle tradizionali categorie esistenti seppur recentemente implementate.

La stessa Corte di giustizia ha ricordato, nella recente sentenza oggetto di disamina, che le norme europee pongono numerosi obblighi positivi in carico ai governi nazionali, quali ad esempio l'adozione di misure giuridiche dirette a tutelare la vita privata e familiare, la protezione del domicilio e delle comunicazioni, ma anche la tutela dell'integrità fisica e psichica delle persone, nonché il divieto di tortura e di trattamenti inumani e degradanti: ai governi nazionali spetta, quindi, conciliare i vari interessi legittimi con i diritti "in gioco" tenendo sempre bene a mente come nessun obiettivo d'interesse generale

---

[48] Per analoghe considerazioni relativamente al tema della *digital evidence* v. ampiamente MARAFIOTI, *Digital evidence e processo penale,* in *Cass. pen.,* 2011, 12, 4509.

[49] D'altra parte, l'impiego dei relativi "risultati" acquisiti nel corso delle indagini, rappresenta uno dei profili più problematici del sistema processuale, sul quale si debbono misurare le scelte valoriali di fondo dell'ordinamento. Per un approfondimento dei divieti di utilizzabilità soprattutto con riferimento alle intercettazioni (art. 271 c.p.p.), sia per meglio esaminare i limiti alla trasmigrazione delle captazioni in procedimenti diversi da quelli in cui sono state disposte (art. 270 c.p.p.) v. GALANTINI *L'inutilizzabilità dei risultati,* in *L'intercettazione di comunicazioni*, a cura di Bene, Bari, 2018, 227.

[50] D'altra parte è indubbio che le indagini, oltre a pesare sul giudizio, abbiano la capacità di influenzare diritti individuali anche diversi da quelli legati all'accertamento giudiziario; pertanto ed a maggior ragione, la relativa "raccolta indiziaria" non può e –sia concesso aggiungere– non deve muoversi con la eccessiva fluidità con cui invero pare muoversi. Così SCALFATI, *Il fermento pre-investigativo,* in *Pre-investigazioni (Espedienti e mezzi),* a cura di Scalfati, Torino, 2020, 4.

può essere perseguito senza tener conto dei i diritti fondamentali interessati dalla misura.

Rebus sic stantibus è difficile prevedere che nella attuale situazione, protesa sia alla gestione della emergenza sanitaria per il Covid 19, sia a quella della triste Guerra in Ucraina, il Parlamento si occupi sollecitamente e nuovamente a mettere in atto una riforma in materia; ciò purtuttavia sarebbe auspicabile per risolvere ogni "criticità applicativa" in tema di *data retention* sulla base dei princìpi elaborati dalla Corte di giustizia UE.