UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di Diritto Privato e Critica del Diritto

Corso di Laurea Magistrale in

Giurisprudenza

Anno Accademico 2023/2024

LA DISCIPLINA PREVISTA DALL'ART. 132 CODICE *PRIVACY*, TRA CRITICITÀ SISTEMATICHE E NOVELLE

Relatrice: Prof.ssa Silvia Signorato

Laureanda: Sara Rossetti

Matricola: 1221297

Sommario

Introduzione **7**

CAPITOLO 1 ..... **11**

1. 1 La nascita del concetto di *privacy* **11**

1. 2 Il concetto di *privacy* in Europa **13**

1. 3 La Direttiva 95/46/CE sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati **16**

1. 4 La cosiddetta Direttiva *"e-privacy"* relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche..... **21**

1. 5 Il d. lgs. 30 giugno 2003, n. 196 (cd. codice *privacy*)..... **25**

1. 6 La cosiddetta Direttiva "Frattini" e la pronuncia "*Digital Rights Ireland*" **28**

1. 7 Cenni al Regolamento Generale sulla protezione dei dati personali e altre Direttive in tema di trattamento dei dati personali svolti nelle attività di indagine per il perseguimento di reati. **34**

CAPITOLO 2 ..... **37**

2. 1 Il d. lgs. 10 agosto 2018, n. 101 e le perplessità sollevate in termini di acquisizione dei dati da parte dell'autorità giudiziaria **37**

2. 2 La sentenza della Corte di Giustizia dell'Unione Europea C- 746/18, del 2 marzo 2021 ..... **42**

2. 3 Il d. lgs. 30 settembre 2021, n. 132 e la questione di illegittimità costituzionale **47**

2. 4 Ulteriori criticità del d. lgs. 30 settembre 2021, n. 132: la mancata predisposizione di un limite soggettivo all'acquisizione dei dati, il profilo della determinazione dei reati presupposto e il problema della figura del Pubblico Ministero **51**

2. 5 La conversione in legge del d. lgs. 30 settembre 2021, n. 132 e l'applicazione ai procedimenti in corso **57**

2. 6 La sentenza della Corte di Giustizia C-178/22 del 30 aprile 2024 .....**62**

CAPITOLO 3 .....**67**

3. 1 Le tempistiche di conservazione e di acquisizione dei dati **67**

3. 2 Il rapporto con il principio di ragionevole durata del processo **72**

3. 3 Il controllo del giudice: profili di incompatibilità della figura dei G.i.p. a seguito del d. lgs. 30 settembre 2021, n. 132 .....**76**

3. 4 Potere discrezionale del giudice in relazione al criterio della gravità dei reati previsto dal d. lgs. 30 settembre 2021, n. 132. Uno sguardo al commento dell'Avvocato Generale *Collins* **81**

3. 5 Equilibrio necessario (ma possibile?) tra esigenze di sicurezza nazionale e diritto alla *privacy* **85**

3. 6 Il problema dell'inutilizzabilità dei dati di traffico telefonico e telematico e dell'inutilizzabilità della "prova incostituzionale" alla luce della recente giurisprudenza……**92**

3. 7 Natura giuridica e principi costituzionali in comune con la disciplina delle intercettazioni ……..**103**

3. 8 Ulteriore riflessione sul principio di proporzionalità tra "*data retention*" ed intercettazioni ……..**108**

3. 9 Le tipologie di dati interessati dalla "*data retention"* e il problema della base giuridica all'indomani della sentenza della Corte di Giustizia "*Digital Rights Ireland"*……**112**

Conclusioni **117**

Bibliografia…….**119**

Indice delle pronunce…….**127**

Introduzione

Questo elaborato, in prima battuta, esamina la storia del concetto di *privacy* dell'America di fine Ottocento e dell'Europa del secondo dopo guerra. Successivamente, esso ripercorre le più importanti tappe normative europee che hanno regolamentato la disciplina in materia di protezione e trattamento dei dati personali delle persone fisiche.

Vengono analizzate sia direttive europee che interventi legislativi interni secondo un ordine cronologico. L'elaborato propone inizialmente l'analisi della Direttiva 95/46/CE sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e della Direttiva *"e-privacy*" relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche. Con riguardo all'Italia, viene esaminata anche la prima regolamentazione in materia, ovvero il d. lgs. 30 giugno 2003 n. 196, il cosiddetto codice *privacy*.

L'elaborato, inoltre, propone anche l'analisi di importanti interventi giurisprudenziali della Corte di Giustizia dell'Unione Europea. Infatti a seguito dello studio della cosiddetta Direttiva "Frattini", è stata esaminata anche la sentenza della Corte di Giustizia "*Digital Rights Ireland*" che ne ha sancito l'invalidità. Per ragioni di completezza, l'elaborato accenna anche al Regolamento Generale sulla Protezione dei Dati Personali e alle Direttive 680/16/UE e 681/16/UE in tema di trattamento dei dati personali svolti nelle attività di indagine per il perseguimento di reati.

Nel secondo capitolo, l'attenzione si sposta sulle modifiche introdotte dal legislatore italiano in relazione alla disciplina della "*data retention*". *In primis*, viene esaminato il d. lgs. 10 agosto 2018 n. 101 fornendo una panoramica della disciplina analizzandone anche gli aspetti critici. *In secundis*, si procede all'esame della successiva modifica interna adottata in materia di "*data retention*": il d. lgs. 30 settembre 2021 n. 132 preceduto dall'approfondimento della sentenza della

Corte di Giustizia C-746/18 del 2 marzo 2021. Anche il d. lgs. 30 settembre 2021 n. 132 viene sottoposto ad un'attenta analisi, la quale si preoccupa di rilevarne anche i profili problematici. Conclusivamente, si è poi proceduto allo studio della legge di conversione del decreto sopra citato.

L'ultimo capitolo del presente elaborato analizza tutta una serie di aspetti ritenuti ancor oggi critici, in quanto non disciplinati dalla norma, e confliggenti con alcuni importanti fattori presenti nel nostro ordinamento. Si fa riferimento al problema, non ancora risolto, delle tempistiche di acquisizione e di conservazione dei dati e del possibile conflitto tra la disciplina così delineata e il principio di ragionevole durata del processo. In secondo luogo, si procede con un'analisi della figura del giudice, ad oggi investita del controllo preventivo sulla richiesta delle parti per procedere all'acquisizione dei dati, discutendo la tesi secondo la quale si possa riscontrare una sorta di incompatibilità del G.i.p in relazione alla procedura di archiviazione. Questo capitolo conclusivo prosegue con delle considerazioni circa il potere discrezionale del giudice in relazione al criterio della gravità dei reati introdotto dal d. lgs. 30 settembre 2021, n. 132 e divenuto uno dei presupposti per l'applicazione della procedura di acquisizione, ed inoltre si tratta il problema del raggiungimento di una situazione di equilibrio, necessario ma non ancora conquistato, tra esigenze securitarie in contrapposizione con il diritto alla *privacy*, in quanto diritto fondamentale degli individui.

Infine, effettua un raffronto tra la disciplina della "*data retention*" e la disciplina delle intercettazioni, analizzandone alcuni aspetti importanti: la sanzione della inutilizzabilità, con una parentesi dedicata alla figura della cosiddetta "prova incostituzionale"; la natura giuridica e i principi costituzionali e sovranazionali comuni ad entrambe le discipline; ed in conclusione, una riflessione sul principio di proporzionalità applicato anche alla disciplina delle intercettazioni.

In conclusione, si tratta, più nello specifico, le tipologie di dati interessati dalla disciplina della "*data retention*" e, per completare l'analisi della normativa, viene

esaminato il problema della base giuridica all'indomani della sentenza "*Digital Rights Ireland*", discutendo dei prossimi interventi futuri del legislatore, comunitario e nazionale.

CAPITOLO 1

1. 1 La nascita del concetto di *privacy*

Il concetto di *privacy* non nasce in Europa, ma negli Stati Uniti, in particolare a Boston, a fine Ottocento. All'epoca, la tecnologia più avanzata era la fotografia, in quanto la radio non era ancora stata inventata. Di conseguenza, il mezzo di comunicazione più diffuso era la stampa.

Il mutamento storico-culturale deriva proprio dall'utilizzo, da parte dei giornali, delle fotografie scattate alle donne dell'alta società di Boston, le quali, grazie alla stampa a rotativa, venivano pubblicate su numerose copie di giornale. Perciò è stato lo sviluppo tecnologico nel mondo della stampa a creare il problema della diffusione, su larga scala, di fotografie raffiguranti soggetti che, inevitabilmente, contenevano anche dettagli sulla loro vita privata.

Il concetto di *privacy*, di cui si comincia a discutere, viene delineato da due giovani avvocati americani, Samuel Warren e Louis Brandeis, in quanto una delle numerose fotografie pubblicate in quegli anni coinvolgeva proprio la moglie di Warren. Di conseguenza, Warren e Brandeis iniziano a ragionare sul possibile danno arrecato non solo alla Signora Warren, ma anche a tutte le altre donne ritratte in queste fotografie.

Dalle riflessioni dei due avvocati, nasce uno scritto pubblicato per la prima volta sulla *Harvard Law Review* nel dicembre del 1890, intitolato "*The Right to Privacy*". Questo saggio, il quale teorizza per la prima volta il *right to privacy*, viene inteso dagli esperti come il punto di partenza del moderno istituto della *privacy*. Warren e Brandeis definiscono per la prima volta il concetto di *privacy* come "*the right to be let alone*", ovvero, il diritto a essere lasciati soli nella propria sfera privata, che va protetta da ingerenze esterne. Infatti, gli autori parlano per la prima volta di invasione della *privacy* con la pubblicazione di fotografie da parte dei giornali, le

quali hanno "invaso il sacro recinto della vita privata e domestica[1]". Per cui, secondo l'impostazione dei due avvocati, la divulgazione indesiderata di "pensieri, sentimenti ed emozioni[2]" potrebbe provocare sofferenza e un senso di inettitudine con conseguenze inevitabili sulle relazioni sociali, sul patrimonio e sugli affari dei soggetti coinvolti.

Il saggio si conclude con una riflessione che collega l'importanza della protezione di suddetti valori con il diritto alla *privacy* appena definito: "…la protezione offerta a pensieri, sentimenti ed emozioni, espressi attraverso la scrittura o l'arte, nella misura in cui consiste nella prevenzione della pubblicazione, è semplicemente esempio dell'applicazione del diritto più generale dell'individuo di essere lasciato solo[3]".

Dunque il concetto di *privacy*, così come delineato da Warren e Brandeis, è stato elaborato, sin dagli albori, secondo una connotazione difensiva[4] dell'individuo e delle proprie informazioni private, proteggendole da illecite diffusioni.

La giurisprudenza americana, di conseguenza, sviluppa una nuova forma di tutela indirizzata alla *privacy*, la quale però si afferma integramente solo negli anni Settanta del secolo scorso. Questa affermazione è avvenuta molto in ritardo perché la *privacy*, così come concepita da Warren e Brandeis, veniva inizialmente vista come un affronto ai valori principali della società americana di quell'epoca. Le Corti americane iniziano a riconoscere, nelle loro pronunce, il diritto alla *privacy*, ma sempre subordinato allo sfruttamento economico e alla ricchezza che i giornali possono ottenere con la diffusione delle fotografie.

---

[1] S. WARREN-L. BRANDEIS, *The Right to Privacy*, in *Harvard Law Review*, dicembre 1890.
[2] S. WARREN-L. BRANDEIS, *The Right to Privacy*, in *Harvard Law Review*, dicembre 1890. In questo passaggio gli autori fanno riferimento all'importanza dell'ordinamento di *common law*, il quale ha reso più semplice ai giudici prevedere una tutela per questi valori senza attendere necessariamente l'intervento del legislatore.
[3] S. WARREN-L. BRANDEIS, *The Right to Privacy*, in *Harvard Law Review*, dicembre 1890.
[4] F. PIZZETTI, *Le sfide della nuova* privacy *nella società digitale e dell'IA*, in *Agenda Digitale*, febbraio 2023, p. 3.

Successivamente, ulteriori dubbi manifestati dalla Corte Suprema derivavano dalla lotta alle forme di criminalità organizzata esistenti all'epoca, con particolare riferimento al proibizionismo. I giudici della Suprema Corte temevano che, una maggiore affermazione del diritto alla *privacy* con conseguente limitazione dei mezzi pubblici di indagine e di repressione di queste forme di criminalità, avrebbe reso più difficoltoso il mantenimento dell'ordine pubblico.

Il cambiamento che ha portato la giurisprudenza americana a modificare la concezione del *right to privacy* e ad accoglierlo così come inteso anche da Warren e Brandeis, è iniziato negli anni Trenta e si è concluso, appunto, negli anni Settanta. Dovuto principalmente allo sviluppo tecnologico, questo mutamento ha comportato un aumento delle cause giuridiche relative alla diffusione di immagini o informazioni private, portando all'attenzione delle Corti americane la necessaria tutela del diritto alla *privacy*, messa costantemente in pericolo dai nuovi strumenti di comunicazione di massa. Tutti i dubbi precedentemente sollevati vengono così risolti con l'affermazione del *right to privacy* anche a livello costituzionale[5], arrivando ad una completa definizione del diritto alla *privacy*.

1. 2 Il concetto di *privacy* in Europa

Il concetto di *privacy* in Europa si sviluppa con un significato diverso. Il contesto socio-culturale, differente rispetto allo scenario americano, innesta negli individui la preoccupazione di possibili interferenze nella loro sfera privata, non da organi di

[5] Caso *Griswold vs Connecticut*, deciso il 7 giugno 1965, nel quale il giudice Douglass individua l'esistenza di un diritto alla *privacy* costruito su specifiche garanzie inizialmente previste per la proprietà. Secondo questa impostazione prevalente, il diritto alla *privacy* risulta essere un "diritto implicito come fondamento di diritti scritti". Emerge un'altra impostazione del giudice Black, il quale afferma che la Costituzione non prevede il diritto alla *privacy*, ma solo una serie di garanzie specifiche, per cui non ci si deve avventurare nella enucleazione di nuovi diritti. La sentenza è importante perché ha permesso di ricavare un diritto non previsto nella Costituzione, grazie al richiamo a diverse sentenze precedenti.

stampa, ma dallo Stato. Di conseguenza la *privacy* nasce come strumento di protezione da possibili ingerenze del potere pubblico statale visto che, le idee degli Stati Totalitari, seppure appena caduti, sono ancora presenti in tutta l'Europa post-bellica.

Nell'evoluzione sociale del contesto europeo tra il secondo dopoguerra e l'inizio della Guerra Fredda, la prima importante tappa per il riconoscimento del diritto alla *privacy* è stata l'emanazione di due norme fondamentali: l'art. 8 della CEDU[6] e l'art 2 della Costituzione italiana[7]. Il primo sancisce, a livello internazionale, il diritto al rispetto della vita privata ed è ritenuto, dalla dottrina[8], "il punto di arrivo di un processo di codificazione e costituzionalizzazione del diritto alla *privacy*"[9], mentre il secondo prevede il rispetto dei diritti inviolabili dell'uomo con l'accentramento della figura del cittadino rispetto allo Stato. Nello specifico, l'Italia disciplina in maniera indiretta il diritto alla *privacy* all'interno della Costituzione. È possibile, infatti, ricavarlo grazie alla lettura degli artt. 14, 15, e 21, i quali concernono rispettivamente il domicilio, la libertà e la segretezza della corrispondenza e la libertà di manifestare liberamente il proprio pensiero. Questo orientamento è stato superato da una sentenza della Corte Costituzionale[10], la quale è intervenuta, in maniera esplicita, inserendo così il diritto alla *privacy* tra i diritti inviolabili previsti all'art. 2 della Costituzione[11].

[6] Convezione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali, firmata a Roma, 4 novembre 1950 e ratificata con l. del 4 agosto 1955, n. 848.
[7] Costituzione della Repubblica Italiana, promulgata il 27 dicembre 1947 ed entrata in vigore il 1°gennaio 1948.
[8] Per approfondimenti sull'art. 8 CEDU, O. POLLICINO-M. BASSINI, *Commento all'art. 8 CdfUE*, in R. MASTROIANNI-O. POLLICINO-S. ALLEGREZZA-F. PAPPALARDO-O. RAZZOLINI (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Giuffrè, 2017.
[9] Cit. F. ROSSI DAL POZZO, *La tutela dei dati personali nella giurisprudenza della Corte di giustizia*, in *Eurojus*, 2018, p. 10.
[10] Corte Cost. 38/1973.
[11] C. RECCHIA-F. SCORZELLI, Privacy*: il nuovo pacchetto di normativa europea per la protezione dei dati personali*, in *Annunziata&conso*, 2017, p. 2 e ss.

Il primo stato europeo ad introdurre una legge per la protezione dei dati personali è la Germania Federale[12] nel 1978. Questa norma nasce in risposta al costante controllo sui cittadini, ancora presente nella Germania dell'Est, da parte dell'Unione Sovietica, per reagire al pericolo della dittatura. Nello specifico, la norma serve ad evitare che lo Stato, trattando i dati personali dei cittadini, rafforzi la sua dittatura.

Negli anni Ottanta, con lo sviluppo tecnologico e la diffusione dell'informatica di massa, il Consiglio d'Europa adotta la Convenzione 108[13] che diventa così il documento più importante a livello europeo sulla protezione dei dati personali. Si applica a tutti i trattamenti di dati personali effettuati sia nell'ambito privato che pubblico. Lo scopo della norma è proteggere gli individui da possibili abusi prevedendo anche le modalità con cui deve avvenire la raccolta dei dati personali. Essi devono essere trattati per specifici scopi e non devono essere destinati ad un uso incompatibile con la finalità di trattamento originaria.

Con la creazione della Comunità Europea e l'istituzione del Mercato Unico Europeo, ne è derivato il problema dell'introduzione di una normativa unitaria a livello europeo sulla protezione dei dati personali. Bisognava individuare uno strumento normativo che potesse armonizzare le scelte adottate nei singoli Stati per evitare da un lato le norme troppo flessibili, le quali avrebbero potuto causare una polarizzazione da parte degli Stati, e dall'altro le norme eccessivamente rigide, le quali avrebbero impedito ai dati di circolare. Per cui, tra le Direttive e i Regolamenti che sono due dei più importanti atti giuridici della Comunità Europea, la scelta ricadde sullo strumento della Direttiva.

[12] In particolare, il Land dell'Assia.

[13] "Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale", entrata in vigore il 28 gennaio 1981. Successivamente nel 2018, il Consiglio adotta un protocollo di aggiornamento della normativa, denominato Convenzione 108 +, con l'intento di fornire un quadro giuridico che faciliti il flusso di dati.

1. 3 La Direttiva 95/46/CE sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati

Siamo quindi alle origini della disciplina sulla protezione dei dati personali e gli Stati non avevano ancora adottato norme specifiche e complete, per cui si scelse di emanare una Direttiva, in quanto il Regolamento, immediatamente vincolante senza atti di recepimento, era ritenuto troppo rigido. La Direttiva, invece, era vincolante per gli Stati nell'indicazione dei fini e degli obiettivi da raggiungere, ma per quanto riguardasse i mezzi questi erano scelti esclusivamente dai legislatori nazionali.

Il Parlamento e il Consiglio, dunque, hanno adottato la direttiva 95/46/CE[14] sulla protezione dei dati personali con lo scopo di promuovere un elevato livello di tutela dei diritti fondamentali dei cittadini. Gli Stati, con proprie leggi di recepimento, avevano il compito di adottare una normativa che garantisse un livello elevato e uniforme di tutela dei diritti e delle libertà dei cittadini.

Essendo stata adottata a seguito della regolamentazione del Mercato Unico Europeo, la Direttiva aveva come riferimento la regolazione degli scambi commerciali e questo si evince dalla lettura della stessa, nella quale i dati personali vengono così concepiti come all'interno di una relazione tra titolare e interessato. In questa visione il dato era di proprietà dell'interessato per cui non poteva essere utilizzato da nessuno senza il suo consenso[15]. Per questo motivo, la Direttiva 95/46/CE fu vista per molto tempo solo come un adempimento burocratico in un'ottica di armonizzazione del mercato.

Esaminando più nel dettaglio la Direttiva, l'art. 1 faceva riferimento all'oggetto della stessa, con particolare attenzione alla tutela della vita privata degli individui: "Gli Stati membri garantiscono, conformemente alle disposizioni della presente Direttiva, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e

[14] Direttiva 1995/46 del Parlamento Europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.
[15] Per la prima volta si parla di consenso con riferimento ai dati personali.

particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali"[16].

Inoltre la Direttiva ha introdotto le autorità di controllo indipendenti[17] per l'esercizio dell'attività di verifica sulla corretta attuazione di queste regole da parte dei singoli Stati.

Un'altra importante regolamentazione prevista dalla Direttiva riguardava il trasferimento dei dati personali al di fuori dello Spazio Economico Europeo, il quale era vietato se lo Stato di destinazione non avesse previsto delle regole a protezione dei dati dello stesso livello previsto dalle norme europee. A differenza della Convenzione 108, la Direttiva adotta una visione opposta a protezione di attività esercitate in Europa, da ingerenze esterne. Ecco spiegata l'impostazione appena discussa sul divieto di trasferimento di dati con paesi che non garantivano una protezione che rispettasse gli standard equivalenti a quelli europei.

È interessante notare come la Direttiva, all'art. 33, prevedeva la possibilità per la Commissione di presentare una relazione al Parlamento e al Consiglio sull'applicazione della stessa con il suggerimento, eventuale, di opportune proposte di modifica. Nella presente relazione[18], la Commissione ha effettuato un esame concernente le misure di attuazione della Direttiva adottate dai singoli Stati membri e ha aperto un dibattito pubblico visto anche la rapida evoluzione delle tecnologie nella società.

La Commissione ha ribadito la natura prettamente commerciale della Direttiva, la quale traeva origine dalla necessaria integrazione europea anche in termini di scambi commerciali e circolazione dei dati tra gli Stati membri, in quanto le differenti normative interne previste dai singoli Stati causavano difficoltà al trasferimento dei dati. È stata affermata poi la "vasta incidenza[19]" della Direttiva:

[16] Art. 1 Dir. 95/46/CE
[17] Ovvero i Garanti.
[18] Relazione COM (2003) 265 sull'applicazione della direttiva sulla tutela dei dati (95/46/CE).
[19] Relazione COM (2003) 265 sull'applicazione della direttiva sulla tutela dei dati (95/46/CE), p. 3.

nonostante il suo scopo giuridico fosse circoscritto all'ambito economico-commerciale, i suoi effetti e la sua applicazione riguardavano ogni cittadino, in quanto "persona interessata"[20].

Il dibattito aperto dalla Commissione in sede di revisione della presente, coinvolgeva amministrazioni pubbliche, istituzioni, associazioni di imprese e di consumatori, singole imprese e infine anche i cittadini. La Commissione ha presentato una serie di quesiti alle parti coinvolte, tramite questionari pubblicati sul suo sito Web, e ha commissionato studi alle migliori università. Il dibattito ha avuto esito positivo per quanto concerne i rappresentanti delle imprese e delle amministrazioni pubbliche, i quali hanno partecipato attivamente al dialogo dando anche spunti ulteriori per garantire un efficace tutela dei diritti personali in questione[21].

All'esito del dibattito e della revisione da parte della Commissione, è emerso come una modifica alla Direttiva non sarebbe stata opportuna, in quanto pochi partecipanti al dibattito avevano presentato richieste di modifica, comunque circoscritte ad un numero ristretto di disposizioni. La Commissione era concorde con questa impostazione e ha presentato, nel corso della relazione, le ragioni per le quali una modifica della Direttiva sarebbe risultata non indicata.

Inizialmente, ha fatto riferimento alla limitata applicazione della stessa, in quanto solo pochi Stati l'avevano recepita entro i termini indicati, mentre in alcuni paesi è mancata proprio la legge di attuazione[22]. È ritenuta questa la ragione principale per cui una proposta di modifica sarebbe stata inadeguata.

Inoltre, la Direttiva presentava degli strumenti che consentivano di risolvere le difficoltà sollevate nel corso del dibattito senza ricorrere ad una modifica *in toto* della stessa. La maggior parte delle difficoltà riscontrate derivavano da una scorretta

[20] Relazione COM (2003) 265 sull'applicazione della direttiva sulla tutela dei dati (95/46/CE), p. 4.
[21] D'altra parte, vi è stata limitata partecipazione delle organizzazioni dei consumatori.
[22] La maggior parte degli Stati membri ha notificato solo tra il 2000 e il 2001.

attuazione delle norme previste dalla Direttiva da parte degli Stati in sede di attuazione, con la conseguenza che sarebbe stato compito dei singoli stati apportare le dovute modifiche. Ulteriori discrepanze individuate erano causate dalle differenti prassi in capo agli Stati membri, per le quali la Direttiva disponeva di strumenti che favorivano la collaborazione tra le autorità dei singoli paesi, senza ricorrere ad un emendamento.

La Commissione ha espresso il suo parere positivo anche in relazione all'obiettivo di favorire la libera circolazione dei dati personali. Ha evidenziato inoltre come, dopo l'adozione della Direttiva, non sia mai stato portato all'attenzione della Commissione nessun caso di ostacolo al trasferimento dei dati personali tra gli Stati membri. Per quando concerne il livello di protezione dei suddetti dati, la Commissione si riteneva soddisfatta in quanto certificava che fosse stato raggiunto uno standard di protezione tra i più elevati.

Però, la Commissione ha espresso anche pareri negativi. In particolare, con riferimento agli interventi eseguiti dai rappresentanti delle imprese, era emersa la difficoltà di questi ultimi di "sviluppare politiche paneuropee in materia di tutela dei dati"[23] proprio a causa di alcune disparità derivanti dalla Direttiva. La Commissione concordava con questa visione e ricordava come la Direttiva stessa proponesse un avvicinamento delle legislazioni dei vari Stati e non una completa uniformità. Era opportuno, anche secondo la Commissione, che gli interessati puntassero ad una maggiore convergenza delle legislazioni, auspicando una omogeneità sia con riferimento alle modalità di applicazione delle indicazioni in materia, sia sugli interventi delle autorità nazionali di controllo.

In relazione a particolari divergenze individuate tra la Direttiva e le normative di attuazione dei singoli Strati, la Commissione si è espressa come segue: in generale la maggior parte delle divergenze non costituivano violazione della normativa

[23] Relazione COM (2003) 265 sull'applicazione della direttiva sulla tutela dei dati (95/46/CE), p. 13.

comunitaria; invece, le restanti differenze impedivano la creazione di un sistema di regolamentazione semplificato tra gli Stati, per cui costituivano motivo di costante controllo da parte della Commissione.

La revisione si conclude con un augurio da parte della Commissione che auspica una migliore applicazione della Direttiva 95/46/CE e una sua esecuzione più semplificata e uniforme nella maggior parte degli Stati membri. La Commissione, infine, attende che siano i singoli Stati ad apportare le necessarie modifiche per conformarsi al dettato della Direttiva e, per ultimo, incoraggia i cittadini ad avvalersi dei diritti conferiti loro.

Questa Direttiva è stata ritenuta dalla dottrina incompleta in relazione alla protezione *in toto* del diritto alla *privacy*. Nello specifico, si riteneva che la suddetta Direttiva fosse caratterizzata da validi e importanti principi, rispettati dalla stessa, ma, inoltre, si evidenziava come la sua impostazione, così generica, avesse causato una serie di frammentazioni applicative tra i vari Stati, a discapito della ricerca della necessaria applicazione omogenea della disciplina a protezione del diritto alla *privacy* su tutto il territorio dell'Unione Europea[24].

In conclusione, l'iter europeo della costruzione della normativa in materia di *privacy* iniziato con la Direttiva 95/46/CE ha necessitato di ulteriori modifiche normative. Queste modifiche si erano rese necessarie data la continua evoluzione dei mezzi di comunicazione elettronica e della tecnologia, tenendo conto lo sviluppo, iniziato in quegli anni, dell'accesso ad *Internet*. In particolare fu evidenziato come non fosse ancora stato trattato il tema della riservatezza, della vita privata e della protezione dei dati dei cittadini. Era necessario, quindi, procedere con l'individuazione di una normativa che, a livello europeo, prevedesse una forma di protezione contro i nuovi pericoli dei dati personali.

[24] C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *federalismi.it*, *Riv. dir. pub.*, 2018, p. 3 e ss.

1. 4 La cosiddetta Direttiva *"e-Privacy"* relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche[25]

Con questa Direttiva[26], il legislatore europeo ha inteso armonizzare le singole normative interne degli Stati con lo scopo di individuare una normativa che assicurasse un alto standard di protezione dei diritti e delle libertà fondamentali, con esplicito riferimento in questo caso al diritto alla vita privata. Visto l'avvento di *Internet*, il quale ha disorientato i cittadini offrendo una nuova visione di mercato, si è reso necessario disciplinare queste nuove possibilità offerte dal *Web*, le quali rappresentavano possibili pericoli per i dati personali dei soggetti.

Le disposizioni di questa Direttiva integrano le prescrizioni previste nella precedente Direttiva 95/46/CE, la quale continuerà ad essere applicata in riferimento alla tutela dei diritti e delle libertà fondamentali non specificatamente previsti nella Direttiva in esame e in relazione ai ricorsi giurisdizionali, alle responsabilità e alle sanzioni previste.

In particolare, la Direttiva 2002/58/CE riprende un requisito fondamentale, introdotto precedentemente dalla Direttiva 95/46/CE: il consenso. Definito e circoscritto inizialmente come un consenso prestato esclusivamente al trattamento dei dati personali, viene successivamente ampliato ed inteso come "qualsiasi modalità appropriata che consenta all'utente di esprimere liberamente e in conoscenza di causa i suoi desideri specifici, compresa la selezione di un'apposita casella nel caso di un sito *Internet*"[27].

---

[25] Dir. 2002/58 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, definita Direttiva *e-Privacy.*

[26] La quale ha abrogato la direttiva 97/66, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle telecomunicazioni resa obsoleta dati gli sviluppi nei campi della tecnologia e dei servizi di comunicazione elettronica.

[27] Considerando 17, Dir. 2002/58/CE. Si noti il costante riferimento al mondo del *Web*, divenuto uno strumento di comunicazione importante. Il consenso, dunque, diventa fondamentale anche per la navigazione in *Internet*, il quale contiene molti pericoli per i dati personali.

I due aspetti più importanti introdotti dalla Direttiva, qui esaminata, riguardano la sicurezza dei dati e il regime della loro riservatezza. È opportuno quindi, concentrarsi su questi per procedere ad un'analisi completa degli aspetti fondamentali di questo intervento normativo europeo.

All'art. 4 della Direttiva 2002/58/CE, il legislatore individua quelle che sono le attività e le misure[28] che i fornitori dei servizi di comunicazione devono adottare per la salvaguardia dei dati personali. Si assicura così uno standard ritenuto dal legislatore stesso "adeguato al rischio esistente"[29]. Se invece, vi è il pericolo di un particolare tipo di violazione della sicurezza dei dati in rete, i fornitori dei servizi di comunicazione sono obbligati, in base a quanto previsto dalla Direttiva[30], ad informare gli utenti del rischio e inoltre, qualora le misure adottate non bastassero ad arginare la possibile violazione, devono indicare loro tutti i possibili rimedi attuabili con l'indicazione dei relativi costi.

I rischi a cui la Direttiva fa riferimento riguardano non solo i pericoli che i servizi di comunicazione possono riscontrare in una rete aperta come *Internet*, ma anche i pericoli che si possono presentare in ambito telefonico, e quindi analogico.

È necessario, inoltre, prevedere delle misure che prevengano l'accesso non consentito in riferimento alle comunicazioni tra utenti. La riservatezza è un elemento importante per il mantenimento della segretezza delle comunicazioni elettroniche realizzate ricorrendo a reti di comunicazioni pubbliche. Perciò l'art. 5, par. 1 della Direttiva prevede che gli Stati, nelle loro disposizioni interne, disciplinino la riservatezza delle comunicazioni effettuate tramite l'intervento dei servizi di comunicazione pubblica. In particolare, la Direttiva afferma che vengono

[28] Si fa riferimento a misure sia tecniche che organizzative. Ad esempio attraverso l'uso di programmi informatici o tecniche di criptaggio.
[29] Art. 4, par. 1, Dir. 2002/58/CE.
[30] Art. 4, par. 2, Dir. 2002/58/CE.

vietati "l'ascolto, la captazione, la memorizzazione e altre forme di intercettazione o di sorveglianza della comunicazioni e dei relativi dati del traffico…"[31].

Questa Direttiva è stata sottoposta, nel 2008, ad una procedura di riesame. Questa proposta di revisione derivava dal Gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali[32], il quale, a seguito di una consultazione pubblica aperta dalla Commissione, ha presentato una richiesta di revisione della Direttiva con lo scopo di rafforzare la disciplina con regole di sicurezza più rigorose.

Il parere del Gruppo riportava alcune delle riflessioni sostenute dal Garante italiano[33] per la protezione dei dati personali. I maggiori Garanti europei concordavano sulla necessità di disciplinare il fenomeno della protezione dei dati con una accezione più ampia, in quanto la natura delle reti di comunicazione si è fatta sempre più mista, cioè pubblica e privata.

Successivamente, il Gruppo è intervenuto proponendo alcuni emendamenti di modifica della Direttiva, con riferimento all'estensione ai fornitori dei servizi di comunicazione dell'obbligo di notificare le violazioni della sicurezza a tutti gli utenti, senza distinguere più tra abbonati e non abbonati[34]. Secondo la loro impostazione, questa estensione garantirebbe una riduzione dei rischi per gli utenti e una maggiore assunzione di responsabilità da parte dei fornitori dei servizi.

Questa proposta di modifica della Direttiva è stata successivamente bocciata dalla Commissione e dal Parlamento europeo. A parere di chi scrive, si ritiene che questa

---

[31] Art. 5, par. 1, Dir. 2002/58/CE.

[32] Istituito in virtù dell'art. 29 della Dir. 95/46/CE. È un organo consultivo indipendente per la protezione dei dati personali e il diritto alla riservatezza.

[33] Parere 2/2008 del Garante della *Privacy* sul riesame della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, adottato il 15 maggio 2008.

[34] Può infatti accadere che nei confronti di un soggetto che ha disdetto il suo abbonamento, i suoi dati siano ancora in possesso del responsabile del servizio di comunicazione. Questa modifica risulterebbe utile anche con riguardo a terze persone, di cui i fornitori posseggono alcune informazioni, che non sono abbonate.

proposta non abbia ottenuto seguito, proprio perché ricorrere ad una modifica di una Direttiva non era ritenuto, sia dalla Commissione sia dal Parlamento, la modalità migliore per facilitare gli Stati a recepire, in un secondo momento, queste modifiche. Questa modifica avrebbe dato vita ad una disciplina ancora più frammentata, distante quindi da quel ideale di unità che l'Europa si era prefissata sin dal perfezionamento del concetto di *privacy*.

Con riferimento alla disciplina della "*data retention*", ovvero la raccolta e la conservazione dei dati da parte dei servizi di comunicazione per la repressione dei reati, la Direttiva 2002/58/CE è la risposta europea agli attentati dell'11 settembre 2001. A seguito di questa tragedia, l'orientamento dei legislatori, europei e internazionali, passò da una tendenza "*privacy oriented"* ad una a protezione di altri diritti come la sicurezza pubblica e la lotta alla criminalità internazionale. La Direttiva *e-Privacy*[35] prevedeva, all'art. 5, un divieto generale di memorizzazione e conservazione dei dati di traffico telefonico e telematico. All'art. 6, invece, era previsto l'obbligo per i fornitori dei servizi di comunicazione, responsabili anche della conservazione, di cancellare suddetti dati, oppure renderli anonimi, qualora non fossero più necessari ai fini della trasmissione della comunicazione. Ed infine, all'art. 15, la Direttiva prevedeva una eccezione secondo la quale, gli Stati potevano adottare misure alternative che limitassero i diritti e gli obblighi disciplinati dalla stessa, però solo dove questa limitazione risultasse idonea, necessaria e, soprattutto, proporzionata all'attività di salvaguardia della sicurezza nazionale di repressione dei reati. Infatti, è opinione prevalente quella secondo la quale la normativa interna di uno Stato non possa stabilire, in maniera arbitraria, una disciplina a favore della sicurezza e a discapito del diritto fondamentale alla *privacy*, dovendo ricorrere ad un necessario bilanciamento tra i due interessi coinvolti[36].

[35] Cosi era denominata la Direttiva 2002/58/CE.

[36] G. FORMICI, *Tutela della riservatezza delle comunicazioni elettroniche: riflessioni (ri)partendo dalla pronuncia* Ministero Fiscal, in *Osservatorio Costituzionale*, 2018, p. 474 e ss.

In conclusione, queste due Direttive costituiscono il primo intervento dell'Europa sulla regolamentazione del concetto di *privacy*. Risulta necessario esaminare le scelte interne adottate dall'Italia a seguito della disciplina delineata da queste due Direttive.

1. 5 Il d. lgs. 30 giugno 2003, n. 196 (cd. codice *privacy*)

A seguito delle Direttive 95/46/CE e 2002/58/CE, l'Italia ha recepito tutte le indicazioni all'interno di singole e frammentate disposizioni[37] sul trattamento dei dati personali. A causa della complessità della materia, si è reso necessario un intervento legislativo che creasse un testo unico contente tutte le disposizioni in materia di trattamento e protezione dei dati personali. Pertanto fu emanato, nel giugno del 2003, il codice in materia di protezione dei dati personali[38].

Il codice *privacy* è caratterizzato, dal punto di vista strutturale, da tre sezioni: la prima riporta tutte le definizioni di base e le regole generali in riferimento al trattamento dei dati; la seconda parte specifica l'ambito di applicazione del codice; infine la terza parte disciplina la struttura e le funzioni della figura del Garante per la protezione dei dati personali e stabilisce quali sono gli strumenti di protezione in capo al soggetto che subisce una lesione del diritto alla riservatezza.

Nella redazione del codice, il legislatore ha seguito lo scopo di individuare un equilibrio solido tra gli interessi del titolare del trattamento, ovvero il gestore del servizio di comunicazione, e l'interessato, ovvero il soggetto a cui si riferiscono i dati. Di conseguenza anche in Italia, il concetto di *privacy* viene maggiormente circoscritto e disciplinato, sotto un punto di vista innovativo, come

[37] Ad esempio, la lg. 675 del 31 dicembre 1996 rubricata "tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali".
[38] D. Lgs. 196 del 30 giugno 2003, denominato Codice in materia di protezione dei dati personali. Entrato in vigore il 1° gennaio 2004.

autodeterminazione del soggetto a livello informatico e digitale e come strumento di controllo e di protezione dei dati personali.

L'obiettivo del legislatore è quello di impedire che i dati personali di un soggetto vengano trattati illecitamente, quindi senza il suo consenso, arrecandogli così un pregiudizio. La disciplina così impostata crea per la prima volta, a livello interno, una relazione tra diritto alla riservatezza di un utente in un'ottica di scambio di informazioni a livello informatico, e diritto alla protezione dei suddetti dati.

Il codice *privacy* è stato oggetto di numerose modifiche nel 2018[39] a seguito dell'approvazione del Regolamento generale sulla protezione dei dati[40]. I legislatori europei hanno ritenuto ormai le Direttive inadeguate, e di conseguenza hanno approvato il primo Regolamento in materia di protezione dei dati personali. Questo Regolamento, valevole per tutti gli Stati europei in maniera uniforme, sostituisce numerose norme contenute nel codice *privacy*. Infatti, tutte le definizioni rilevanti per la disciplina dei dati personali, sono contenute nel Regolamento, noto anche con la denominazione inglese *"General Data Protection Regulation"*. Ma non solo. Anche le regole riguardanti le condizioni di trattamento dei dati sono, ad oggi, fissate nel Regolamento.

Quello che è importante ricordare è che il Regolamento generale sulla protezione dei dati non interviene proprio su tutto, in quanto alcune questioni sono lasciate alla regolamentazione nazionale. Per cui il codice *privacy*, che definiamo oggi codice novellato a seguito delle modifiche apportate dal Regolamento, è stato solo

[39] Dec. lgs. 10 agosto 2018, n. 101. Recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

[40]Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

parzialmente riformato in quanto interviene con riferimento ai punti che il legislatore europeo ha voluto lasciare alla normativa interna[41].

Esaminiamo dunque questi ambiti. La disciplina dell'autorità che garantisce la tutela dei dati personali è interamente prevista a livello nazionale, in quanto un modello unico individuato a livello europeo non sarebbe stato possibile vista la diversità dei singoli Stati. Anche la disciplina delle sanzioni è prevista a livello interno, poiché in virtù del principio di sovranità degli Stati, l'Unione Europea non ha competenze penali. Per cui è lo Stato ad indicare quelle che sono le sanzioni penali che il magistrato[42] dovrà erogare in presenza di violazioni delle norme contenute nel codice novellato.

Un ulteriore elemento che necessita di attenzione, in quanto introdotto, attraverso l'emanazione del codice *privacy*, è l'istituzione dell'Autorità amministrativa denominata Garante della *privacy*. Questa figura, già prevista a livello europeo, è dotata di "carattere politico-amministrativo[43]" con lo scopo di rivestire una funzione di controllo e di repressione, indipendente dai poteri dello Stato. L'idea del legislatore era, appunto, quella di creare un modello normativo, il quale, da un lato, puntasse alla realizzazione di una norma il più completa possibile, mentre dall'altro, desse importanza alle disposizioni attuative del Garante, riconoscendogli i dovuti poteri di vigilanza e di intervento.

Ad oggi quindi il codice *privacy* novellato costituisce un elemento normativo importante per la protezione dei dati personali e la gestione delle regole in materia di trattamento, nonché la normativa di riferimento per lo Stato italiano.

[41] Ricordando che l'Unione Europea stabilisce la "cornice" di principi fondamentali che il legislatore interno deve tenere presente nella stesura della norma.
[42] Le sanzioni vengono erogate dal magistrato in quanto l'autorità Garante è solo un organo amministrativo.
[43] P. TRONCONE, *Profili penali del codice della* privacy, in *Riv. pen*, 2004, p. 1.

1. 6 La cosiddetta Direttiva "Frattini" e la pronuncia "*Digital Rights Ireland*"

Ritornando a livello europeo, la pressione socio-politica derivante dagli attentati terroristici, che nel periodo di tempo compreso tra il 2004 e il 2005 hanno interessato l'Europa, in particolare Londra e Madrid, ha spinto l'Unione Europea ad adottare un'ulteriore regolamentazione della materia. Fu emanata la Direttiva 2006/24/CE[44], definita anche Direttiva Frattini, dal nome dell'allora Ministro degli Affari Esteri.

Questa Direttiva aveva lo scopo, come si evince dalla lettura dell'art. 1, di armonizzare le normative dei singoli Stati relative agli obblighi, per i fornitori di servizi di comunicazione, di conservazione dei dati sia telefonici che telematici, per garantire la fruibilità degli stessi a fini di indagine per l'accertamento e la repressione dei reati gravi. Il requisito della gravità del reato è demandato a ciascuna normativa interna dei singoli Stati.

In relazione alla conservazione dei dati, la Direttiva indica anche, all'art. 5, le sei categorie di dati da conservare[45]. Esaminiamole brevemente. Gli Stati devono provvedere alla conservazione delle seguenti categorie di dati: i dati necessari per rintracciare e indentificare la fonte della comunicazione[46]; i dati necessari per rintracciare e indentificare la destinazione di una comunicazione[47]; i dati necessari

---

[44] Dir. 2006/24 del Parlamento e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la Direttiva 2002/58/CE. Commentata anche da A. CISTERNA, *Attuazione della Dir. 2006/24/Ce riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la Dir. 2002/58/Ce (commento al d.leg. 30 maggio 2018 n. 109)*, in *Guida al Diritto*, fasc. 39, 2008, p. 33.

[45] Recepite dall'Italia con il d. lgs. 30 maggio 2008, n. 109, che ha modificato l'art. 132 del codice *privacy*.

[46] Ci si riferisce al numero di telefono del chiamante, il nome e indirizzo dell'utente e infine l'indirizzo di protocollo *Internet* (IP) in caso di accesso ad *Internet*.

[47] Il numero di telefono del destinatario della chiamata, l'identificativo dell'utente o il numero telefonico nel caso di posta elettronica o telefonia via Internet. Un provvedimento del Garante per la protezione dei dati personali, con un provvedimento del 17 gennaio 2008, ha chiarito in merito alla possibilità di conservare anche l'indirizzo IP. Viene esclusa questa possibilità in quanto la conservazione degli indirizzi IP risulterebbe avere contenuto comunicativo. I fornitori dei servizi di

per determinare l'ora, la data e la durata della comunicazione; i dati necessari per determinare il tipo di comunicazione; i dati necessari per determinare le attrezzature di comunicazione degli utenti o quello che si presume essere le loro attrezzature[48]; infine, i dati necessari per determinare l'ubicazione delle apparecchiature di comunicazione mobile.

Inoltre la Direttiva prevede che queste categorie di dati vengano conservati per un periodo non inferiore a sei mesi e non superiore a due anni dalla data di comunicazione.

Lo scopo armonizzatore[49] della Direttiva "Frattini" attribuisce ai precetti, in essa contenuti, una duplice caratteristica: la specialità della disciplina in virtù di quella generale contenuta nella precedente Direttiva[50] e la sua rilevanza in ambito penalistico e processual-penalistico, in quanto l'obbligo di conservazione dei metadati e la successiva possibilità per l'Autorità pubblica di accedervi, fanno della "*data retention*" uno strumento di indagine di importanza ed utilità molto rilevanti[51].

Alcuni stati europei[52] hanno da subito sollevato dei profili di debolezza della Direttiva. Nello specifico è stata criticata l'impostazione dell'art. 1 della Direttiva, il quale prevedeva che fossero i singoli Stati Membri a definire la categoria di reati, ritenuti gravi, per l'accertamento dei quali i fornitori dei servizi di comunicazione fossero obbligati a conservare i dati; inoltre anche l'art. 4 che consente agli Stati di

---

comunicazione, attualmente, seguono questa impostazione per evitare costi eccessivamente alti e sanzioni potenzialmente serie.

[48] Per la telefonia fissa, ci si riferisce ai numeri telefonici. Per la telefonia mobile, invece, si parla di numeri telefonici, ma anche di codici di identità dei dispositivi: *l'International Mobile Subscriber Identity* (IMSI) e *l'International Mobile Equipment Identity* (IMEI).

[49] Definito così da R. FLOR-S. MARCOLINI, *Dalla* data retention *alle indagini ad alto contenuto tecnologico: la tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato,* Giappichelli, 2022, p. 6.

[50] Si fa riferimento alla Direttiva 2002/58/CE in relazione alla quale la Direttiva "Frattini" raggiunge un grado di specificità maggiore di norme indirizzate al settore delle comunicazioni.

[51]Tenendo anche conto dell'utilità della "*data retention*" come strumento di indagine per l'accertamento e la repressione di reati a sfondo trasnazionale.

[52] Tra questi l'Irlanda.

scegliere i casi, i modi e i soggetti legittimati alla richiesta dei suddetti dati; ed infine le ultime perplessità derivavano dalle tempistiche di conservazione dei dati, indicate dalla Direttiva all'art. 6 e corrispondenti ad un periodo compreso tra i sei mesi e i due anni.

Successivamente, la Commissione presenta al Consiglio e al Parlamento la sua relazione[53] inerente alla valutazione della Direttiva. Questo intervento della Commissione si era reso necessario anche a causa di numerose pronunce di incostituzionalità delle leggi nazionali di attuazione della suddetta Direttiva provenienti da alcuni Stati Membri[54]. Questa relazione sottolinea l'importanza della disciplina della "*data retention*" in ambito investigativo per la repressione dei reati gravi, ma evidenzia la necessità di intervenire, in ottica modificatrice, sulla disciplina degli obblighi di conservazione dei dati con specifico rinvio ai principi di proporzionalità e necessità, con lo scopo di ottenere una disciplina che rafforzi la protezione del diritto alla *privacy*[55].

A fronte di questa impostazione, la Direttiva fu interessata da una importante pronuncia[56] della Corte di Giustizia, la quale è giunta alla conclusione di dichiarare invalida la Direttiva "Frattini". All'attenzione della Corte erano state presentate due cause, poi riunite. La prima causa riguardava la presentazione, da parte della *Digital Rights Ireland*, di un ricorso, dinanzi all'alta corte irlandese, nel quale sosteneva di essere proprietaria di un telefono, utilizzato a partire dal 3 giugno 2006. Il gruppo discuteva la legittimità delle misure adottate sulla conservazione dei dati relativi alle comunicazioni elettroniche e chiedeva, nello specifico, la nullità della Direttiva

[53] Relazione della Commissione al Consiglio e al Parlamento Europeo, COM (2011) 225 definitivo sulla Valutazione dell'applicazione della direttiva sulla conservazione dei dati (direttiva 2006/24/CE), Bruxelles, aprile 2011.
[54] Inizialmente, si parla di Repubblica Ceca, Germania e Romania. Poco dopo anche Bulgaria, Cipro, Ungheria e Slovenia. R. FLOR-S. MARCOLINI, Data retention *e indagini ad alto contenuto tecnologico: la tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato*, Giappichelli, 2022, p. 78.
[55] Relazione della Commissione al Consiglio e al Parlamento Europeo, COM (2011) 225 definitivo sulla Valutazione dell'applicazione della direttiva sulla conservazione dei dati (direttiva 2006/24/CE), Bruxelles, aprile 2011, p. 25.
[56] Corte giust. UE, 8 aprile 2014, cause riunite C-293/12 e C-594/12.

2006/24/CE e della normativa di attuazione interna[57]. Il giudice irlandese, ritenendo di non essere in grado di risolvere la questione del diritto interno senza prima discutere sulla validità della Direttiva, ha così sospeso il giudizio e ha rinviato pregiudizialmente la questione alla Corte. La seconda causa riguardava numerosi ricorsi presentati da altrettanti soggetti[58], i quali chiedevano l'annullamento della legge austriaca sulle telecomunicazioni[59], la quale era a sua volta la trasposizione della Direttiva 2006/24/CE, ritenendo che la legge di attuazione interna violasse il diritto fondamentale dei privati cittadini alla protezione dei propri dati.

La Corte ha rilevato come si tratti di dati che, seppure non riguardino il contenuto delle conversazioni, riportino indicazioni ritenute importanti sulle comunicazioni intrattenute dalle parti. Per cui, l'accesso da parte della pubblica autorità a suddetti dati, comporta una relativa intrusione nella vita privata degli utenti. Inoltre, la Corte ritiene anche che questa ingerenza generi, nei cittadini, l'idea di essere sottoposti costantemente ad un controllo da parte dello Stato e delle sue autorità.

La Corte quindi dichiara la Direttiva 2006/24/CE invalida per violazione del principio di proporzionalità nel bilanciamento tra diritto alla protezione dei dati ed esigenze di sicurezza pubblica. Infatti, l'accesso e la conservazione dei dati, spiega la Corte, si può giustificare con l'obiettivo generale di repressione di gravi forme di criminalità, al quale bisogna sempre contrapporre, in un'ottica di proporzionalità, il rischio di comprimere il diritto fondamentale alla protezione dei dati personali dei cittadini[60]. Ed ecco quindi che la Direttiva indica modalità e tempistiche di conservazione che eccedono i limiti imposti dal principio di proporzionalità, i quali andranno valutati secondo un'attenta analisi per capire entro quali termini si

[57] Si fa riferimento al *Criminal Justice (Terrorist Offences) Act* del 2005.
[58] La sentenza parla di 11128 ricorrenti.
[59] Il riferimento è alla legge austriaca sulle telecomunicazioni introdotta nella legge federale a seguito della Direttiva 2006/24/CE, ovvero la *Telekommunikationsgesetz*.
[60]"I diritti individuali e l'interesse generale sono entrambi meritevoli di tutela e debbono essere garantiti e bilanciati reciprocamente; …". R. FLOR-S. MARCOLINI, *Dalla* data retention *alle indagini ad alto contenuto tecnologico: la tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato,* Giappichelli, 2022, p. 6.

possano limitare i diritti e le facoltà previste in riferimento alla protezione dei dati personali.

Questa pronuncia pone al centro il diritto alla protezione dei dati personali e il principio di proporzionalità, inteso qui come "principio di minima interferenza"[61] nei diritti fondamentali. Proporzionalità che va individuata non più in maniera astratta e differente rispetto a qualsiasi fattispecie criminosa che si contrasti, ma deve essere diversificata e modulata in base al tipo di delitto e alle esigenze investigative ad esso correlate.

Per soddisfare i requisiti individuati dalla motivazione della Corte di Giustizia, la normativa nazionale dovrebbe: *in primis* disciplinare il profilo della conservazione dei dati in maniera chiara e precisa, fissando dei limiti e consentendo così ai soggetti di disporre di sufficienti garanzie a protezione dei dati personali; *in secundis* predisporre di criteri oggettivi alla base della conservazione dei dati, idonei "a delimitare effettivamente la portata della misura[62]".

È interessante soffermarsi sulle considerazioni dell'Avvocato Generale Pedro Cruz Villalon[63] a margine dei procedimenti rinviati alla Corte. Villalon sostiene l'incompatibilità della Direttiva con la Carta dei diritti fondamentali dell'Unione Europea, e in particolare con il, qui disciplinato, diritto alla *privacy*. Nello specifico, l'Avvocato Generale fa riferimento all'incompatibilità solo con l'art. 52 della suddetta Carta, il quale prevede che ogni limitazione all'esercizio dei diritti fondamentali deve essere prevista dalla legge. Legge non rinvenibile nella Direttiva 2006/24/CE poiché non identifica chiaramente i principi che dovrebbero riportare le garanzie minime per la disciplina della "*data retention*".

[61] Cit. R. FLOR-S. MARCOLINI, *Dalla* data retention *alle indagini ad alto contenuto tecnologico: la tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato,* Giappichelli, 2022, p. 6.
[62] R. FLOR-S. MARCOLINI, *Dalla* data retention *alle indagini ad alto contenuto tecnologico: la tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato*, Giappichelli, 2022, p. 82.
[63] Conclusioni dell'Avvocato Generale Pedro Cruz Villalon, presentate il 12 dicembre 2013.

Di conseguenza, Villalon ha affermato che, secondo il suo ragionamento, la Direttiva presentava una duplice natura: da un lato, voleva armonizzare le legislazioni interne degli Stati; e dall'altro, intendeva imporre un obbligo di conservazione dei dati allo scopo di garantirne la diponibilità ai fini di indagini per l'accertamento di reati gravi. Con riferimento al primo aspetto, la Direttiva risultava essere in linea con le precedenti, mentre in relazione alla seconda finalità si riscontravano evidenti problemi di accostamento con il diritto fondamentale della *privacy*.

Esiste, secondo le conclusioni di Villalon, una potenziale lesione del diritto alla *privacy*, sancito all'art. 7 della Carta. Riprese poi dalla Corte nella motivazione della sentenza, si riscontra il rischio che i cittadini siano costantemente, e a loro insaputa, sottoposti ad un controllo da parte delle autorità dei singoli Stati, con conseguente lesione del diritto alla vita privata.

Perciò, l'Avvocato Generale ribadisce la necessità di dichiarare invalida la Direttiva poiché non convince in relazione al mancato rispetto del canone di proporzionalità, in quanto "l'obbligo di conservazione generalizzata imposto dalla normativa comunitaria, costituisce un'ingerenza grave nei diritti dei singoli individui"[64].

In conclusione, ad oggi la Direttiva "Frattini", dichiarata invalida dalla suddetta pronuncia della Corte di Giustizia, non è ancora stata sostituita con una nuova Direttiva. Parte della dottrina[65] definisce questo atteggiamento, tenuto dai legislatori europei e nazionali, di "resistenza[66]" in relazione alla correzione degli elementi di incompatibilità sollevali dalla pronuncia della Corte. Infatti, gli Stati

---

[64] A. MALACARNE-G. TESSITORE*, La ricostruzione della normativa in tema di* data retention *e l'ennesima scossa della Corte di giustizia: ancora inadeguata la disciplina interna?,* in *A. pen.*, 2022, pag. 25.

[65] Ed esempio G. CAGGIANO, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*, in *Nuove tecnologie e diritti umani*, *Saggi*, 2017.

[66] Cit. G. CAGGIANO, *Il bilanciamento tra diritto fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*, in *Nuove tecnologie e diritti umani*, *Saggi*, 2017, pag. 78.

Membri manifestano una sorta di resistenza, ritenuta di forte intensità, a dar seguito alle indicazioni stabilite dalla Corte nell'ottica di un ridimensionamento delle proprie discipline interne, in quanto ritengono la "*data retention*" elemento indispensabile per la sicurezza nazionale[67].

In dottrina, si ritiene che la Corte continuerà ad affermare le proprie interpretazioni a seguito del rinvio pregiudiziale sulla eventuale compatibilità delle normative dei singoli Stati in relazione alla disciplina europea della "*data retention*", con la conseguente creazione di divergenti pronunce interpretative. Dunque, anche in relazione a questa possibile problematica, si auspica un futuro intervento legislativo *in primis* europeo, anche in coordinamento con il Regolamento Generale sulla protezione dei dati personali, seguito successivamente da interventi riformistici nazionali.

1. 7 Cenni al Regolamento Generale sulla protezione dei dati personali e altre Direttive in tema di trattamento dei dati personali svolti nelle attività di indagine per il perseguimento di reati.

A seguito quindi della sentenza *Digital Rights Ireland*, la Direttiva di riferimento per la disciplina della "*data retention*" è tornata ad essere la Direttiva 2002/58/CE. La sua validità è stata ottemperata dall'introduzione del Regolamento Generale sulla protezione dei dati personali, il quale intende fornire maggiore certezza giuridica e semplicità delle norme riguardanti il trattamento dei dati personali.

[67] Per approfondimenti sull'evoluzione della normativa degli Stati Membri, *European Union Agency For Fundamental Rights, Data retention across the EU*, luglio 2017. Nello specifico: "*Member States made only limited progress in adopting new legal frameworks for data retention to incorporate the requirements and safeguards set out in the CJEU's case law. Most seem reluctant to amend their national laws to conform to the Digital Rights Ireland and Tele2 judgments. In the meantime, challenges against domestic data retention laws in Member States generally abated, though three characteristic cases challenging data retention were brought in Germany, the Netherlands and the United Kingdom in 2016*".

Ma nell'ambito della riforma sulla "*data protection"*, iniziata con il GDPR, l'Unione Europea ha previsto la realizzazione di altre due Direttive, le quali si occupano esclusivamente del trattamento dei dati personali in relazione ad indagini svolte per il perseguimento dei reati. Queste due Direttive sono di notevole importanza. Importanza che non è stata rilevata a causa del clamore scatenatosi, successivamente l'emanazione del Regolamento.

La Direttiva 680/16/UE[68] risulta avere disposizioni conformi a quelle previste nel Regolamento, ma con la differenza sostanziale che sono indirizzate ai trattamenti effettuati dalle autorità competenti con lo scopo di svolgere attività di indagine per l'accertamento e la repressione dei reati, di eseguire sanzioni penali e, infine, di salvaguardare la sicurezza pubblica.

Per quanto concerne la Direttiva 681/16/UE[69], invece, essa si occupa del trattamento dei dati con riferimento al codice di prenotazione, definito anche "*Passenger Name Record*". In questo codice troviamo tutti i dati e le informazioni relative al traffico aereo e dei relativi passeggeri. La Direttiva prevede una serie di disposizioni con finalità di prevenzione, accertamento, indagine ed azione penale nei confronti dei reati a matrice terroristica e dei reati gravi[70].

Vi sono delle differenze sostanziali tra le due Direttive. Secondo la Direttiva 680/16/UE il trattamento dei dati può essere eseguito solo da un'autorità competente nelle materie inerenti al trattamento dei suddetti dati[71]. Mentre, in base a quanto previsto dalla Direttiva 681/16/UE, i soggetti che intervengono nel

[68] Dir. 680/16 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati.
[69] Dir. 681/16 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.
[70] I reati gravi a cui si fa riferimento sono contenuti in un elenco allegato alla Direttiva. Vi sono ricompresi sia reati contro il patrimonio sia reati contro le persone fisiche. Si tratta pur sempre di reati che possono avere risonanza internazionale e conseguenze molto gravi per la sicurezza pubblica.
[71] Ad esempio, la Polizia di Stato, la Polizia Postale e la Magistratura.

trattamento dei dati sono differenti, poiché non sono solo le autorità sopra citate, ma anche i singoli vettori aerei che forniscono i dati relativi ai passeggeri e alle loro prenotazioni[72]. Entrambe le Direttive sono state, successivamente, attuate in Italia[73].

Con l'esame di queste Direttive si conclude l'*excursus* sulla regolamentazione della disciplina del concetto di *privacy*, in Europa.

[72] Resta ancora il dubbio se includere o no anche le agenzie di viaggio e gli operatori turistici.
[73] La Direttiva 680/16/CE è stata recepita dall'Italia in data 18 maggio 2018 attraverso il d. lgs. n. 51. Questa norma ha sostituito i titoli I e II della seconda parte del codice privacy. Mentre la Direttiva 681/16/CE fu attuata con il d. lgs. 21 maggio 2018, n. 53.

CAPITOLO 2

2. 1 Il d. lgs. 10 agosto 2018, n. 101 e le perplessità sollevate in termini di acquisizione dei dati da parte dell'autorità giudiziaria

La disciplina della *"data retention*" è stata modificata successivamente all'entrata in vigore del Regolamento Generale sulla protezione dei dati. Il legislatore italiano, nel recepire il Regolamento 2016/679, ha adeguato la normativa nazionale in materia di "*data retention"* alle nuove disposizioni contenute nel suddetto, mediante l'emanazione del d. lgs. 10 agosto 2018, n. 101[74].

Il decreto è entrato in vigore novellando il codice *privacy*. Di conseguenza, ogni pubblica amministrazione, ogni società di servizi, ogni ente ed ogni impresa si è dovuta adattare integralmente alle disposizioni del presente decreto. Dunque tutta la normativa italiana in materia di protezione dei dati personali è da interpretarsi, a seguito dell'emanazione di questo decreto, come appartenente ad un quadro normativo complesso che comprende il Regolamento Generale e il codice *privacy* novellato.

La procedura, che ha portato all'emanazione del d. lgs. 10 agosto 2018 n. 101, è stata molto complessa, in quanto inizialmente si propendeva per una abrogazione totale del codice *privacy* con l'intento di semplificare tutta la disciplina, ma successivamente la scelta è ricaduta su una modifica solo parziale del codice con lo scopo di creare una disciplina armonizzata.

In questo intervento riformistico della disciplina del codice *privacy*, il d. lgs. 10 agosto 2018 n. 101 ha apportato significative modifiche in relazione a norme riguardanti il processo. Modifiche che hanno intaccato anche l'art. 132 codice *privacy* e le relative regole in materia di "*data retention*".

[74] Recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE.

È necessario chiarire che cosa sia la disciplina della "*data retention*". Prevista all'art. 132 codice *privacy*, la disciplina della "*data retention*" prevede la conservazione dei dati di traffico telefonico, telematico e relativo alle chiamate senza risposta da parte dei fornitori dei servizi di comunicazione per l'accertamento e la repressione dei reati.

Il d. lgs. 10 agosto 2018 n. 101, all'art. 11, ha modificato l'originaria impostazione dell'art. 132 codice *privacy*, in particolare ha apportato modifiche ai commi 3 e 5 inserendo anche un comma 5-*bis*. Esaminiamole.

La modifica del comma 3 riguarda l'acquisizione dei dati riferiti alle chiamate in entrata senza risposta. Prima dell'entrata in vigore del decreto, la norma prevedeva una differente disciplina per procedere all'acquisizione dei dati di traffico telefonico provenienti dalle chiamate in entrata e dei dati di traffico telefonico originati dalle chiamate in uscita. La dottrina si è divisa in relazione a questa disciplina differenziata. Parte della dottrina[75] riteneva comprensibile la differenziazione delle chiamate in entrata da quelle in uscita, facendo leva sulla necessità della suddetta differenziazione anche in relazione alla possibile diversificazione degli stessi dati che derivano dalle due forme distinte di chiamata. Mentre, la restante parte della dottrina[76] sostiene la versione opposta, secondo la quale resta oscuro il motivo che abbia portato il legislatore a prevedere una regolazione differenziata, con conseguente maggiore tutela per le chiamate in entrate a discapito delle chiamate in uscita.

Nello specifico, la versione precedente della norma stabiliva che l'acquisizione dei dati delle chiamate in entrata potesse verificarsi solo in presenza di richiesta diretta al fornitore da parte del difensore dell'imputato[77]. La norma fissava anche un requisito per poter procedere con la richiesta di acquisizione dei suddetti dati,

[75] E. ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, Wolters Kluver-Cedam, 2018, p. 131.
[76] A. CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Riv. it. d. proc. pen*, 2005, p. 612.
[77] O anche della persona sottoposta ad indagini.

previsto all'art. 8, comma 2, lettera f[78], il quale stabiliva che fosse necessario dimostrare che la richiesta di acquisizione dei dati in questione, avesse lo scopo principale di prevenire un pregiudizio concreto per le indagini difensive.

In relazione a questa precedente impostazione, è intervenuta la riforma in chiave semplificatrice. Ha eliminato il necessario riferimento alle condizioni per poter procedere alla richiesta di acquisizione, e quindi all'art. 8, comma 2, lettera f, e ha introdotto il concetto di "accesso diretto". Per cui non sarà più necessario attendere che, a seguito dell'istanza del difensore dell'imputato[79], venga emesso un decreto motivato. Per poter quindi procedere all'acquisizione dei dati delle chiamate in entrata, solo nei casi in cui vi sia il rischio di un pregiudizio concreto per il proseguimento delle indagini difensive[80], il difensore procederà alla redazione dell'istanza, senza dover attendere il decreto motivato del giudice.

Veniamo ora alla modifica apportata al comma 5 dell'art. 132 codice *privacy*. La disciplina inizialmente prevista stabiliva che la conservazione e il trattamento dei dati dovesse essere effettuato rispettando le regole a garanzia dell'individuo interessato previsti all'art. 17[81]. La riforma ha eliminato anche questo riferimento e ha stabilito che il trattamento dei dati personali è da effettuarsi con costante rispetto delle direttive fissate dal Garante e individuate all'art. 2-*quinquiedecies*[82], il quale

[78] D. lgs. 10 agosto 2018, n. 101. "…la norma detta una disciplina differente per l'acquisizione del traffico <<in entrata>> e <<in uscita>>. Solo in quest'ultimo caso, infatti, risulta la richiesta del difensore corredata dall'atto di conferimento dell'incarico. Diversamente, nel caso del traffico <<in entrata>> è anche necessario che dalla non acquisizione possa derivare un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397". S. 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, p. 158.

[79] O della persona sottoposta da indagini.

[80] La disciplina delle indagini difensive è prevista dalla lg. 7 dicembre 2000, n. 397.

[81] Codice *privacy*, successivamente abrogato con l'entrata in vigore del d. lgs. 10 agosto 2018, n. 101.

[82] Codice *privacy*.

stabilisce "il trattamento dei dati personali dal rischio elevato in rapporto all'esecuzione dei un compito di interesse pubblico"[83].

La modifica che ha apportato un vero e proprio stravolgimento delle tempistiche di conservazione dei dati da parte dei fornitori dei servizi è stata l'introduzione di un nuovo comma 5-*bis*. Questo comma stabilisce, in un'ottica di contrasto ai fenomeni di terrorismo e in deroga a quanto inizialmente previsto dall'art. 132 codice *privacy*, un termine di settantadue mesi per la conservazione di tutti i tipi di dati, ovvero dei dati di traffico telefonico, dei dati di traffico telematico e dei dati relativi alle chiamate senza risposta, in rapporto all'obiettivo primario di repressione ed accertamento dei reati con finalità di terrorismo e dei reati compresi all'art. 407 c.p.p.

Questa modifica deve essere rapportata con quanto previsto dall'art. 132 codice *privacy* per le altre tipologie di reato. Sulla base di ciò, i fornitori dei servizi di comunicazione sono obbligati a conservare i dati di traffico telefonico per ventiquattro mesi; i dati di traffico telematico per dodici mesi; e, infine, per trenta giorni le chiamate senza risposta. Di conseguenza, i fornitori dei servizi di comunicazione, per evitare di incorrere in inadempimenti, hanno scelto di conservare tutti i dati per un unico termine di settantadue mesi e valutare caso per caso per che tipo di reato si proceda e a che termite sottoporre i dati ad esso riferiti[84].

Questo scaglionamento ha suscitato molte perplessità. È necessario esaminare il profilo dell'acquisizione dei suddetti dati da parte dell'autorità giudiziaria, con riferimento al quale si possono riscontrare delle criticità. Quando quest'ultima presenta richiesta di trasmissione e acquisizione dei dati ai fornitori di comunicazione elettronica, ricade proprio su questi l'obbligo di verificare la compatibilità tra le tempistiche di conservazione e il tipo di reato per cui si procede.

---

[83] S. 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, p. 159.
[84] Per approfondimento, S. 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.

Ne consegue che, siccome i dati vengono conservati necessariamente per settantadue mesi visto le ragioni sopra riportate, e visto che non si può conoscere anticipatamente per che tipo di reato ne verrà richiesta l'acquisizione, nel caso di un dato conservato per ventiquattro mesi di cui ne fosse chiesta la trasmissione superati i mesi sopraindicati anche solo di un giorno, la trasmissione e la successiva acquisizione da parte dell'autorità richiedente sarebbero illegittime[85].

Dal punto di vista prettamente investigativo, le conseguenze potrebbero essere deleterie in riferimento ad un possibile quadro indiziario consolidato, per la maggior parte delle sue risultanze, su dati esterni alle comunicazioni. È quindi possibile che le indagini in ambito penalistico si concentrino sui dati esterni alle comunicazioni e ai c.d. "tabulati", dai quali è possibile rinvenire molteplici informazioni con le quali si può arricchire il materiale probatorio eventualmente già raccolto[86]. L'importanza investigativa dei dati esterni alle comunicazioni è rinvenibile soprattutto quando l'attività di indagine riguarda reati commessi in rete da soggetti non meglio identificati, in quanto "nascosti" dallo schermo del computer o del telefono. Perciò, principalmente in relazione all'attività di repressione di queste forme di illeciti, i suddetti dati e la loro acquisizione rappresentano elementi primari ed essenziali per la costruzione di un solido quadro probatorio. Infatti, l'acquisizione di questi dati viene definita "propedeutica[87]" ad ogni altro adempimento investigativo successivo.

[85]L'inutilizzabilità dei dati di traffico contenuti nei tabulati acquisiti dall'autorità giudiziaria dopo la scadenza del termine previsto per la loro conservazione è data per assodata anche dalla giurisprudenza. Per esempio, Cass., Sez. V, 25 gennaio 2016, n. 7265.
[86]Esistono varie modalità di utilizzo dei tabulati: si possono, ad esempio, utilizzare per individuare l'intestatario di quella utenza telefonica consultando i registri telefonici in capo ai gestori del servizio; inoltre si possono utilizzare per accertare la connessione tra uno o più contatti; ed infine vengono utilizzati per condurre una ricerca accurata nell'area di copertura della cella telefonica "agganciata" da numero telefonico in questione, per capire se l'utente si trovasse in quel dato luogo dove sono avvenuti i fatti. Per approfondimenti, M. VITIELLO, *Celle telefoniche e tabulati: cosa sono e come vengono analizzati nei casi giudiziari*, in *Cybersecurity 360*, 2022, p. 6 e ss.
[87]F. BUCCI, *Data retention: stato dell'arte e sviluppi recenti in Europa*, in *Ius Itinere*, 2020.

Con questa disciplina così regolamentata, il rischio è che venga costruito un quadro indiziario e probatorio sulla base di un dato, importante dal punto di vista investigativo, ma che sia frutto di una illegittimità causata dalla scadenza dei termini per la sua conservazione. Illegittimità derivante dal mancato controllo da parte dei fornitori dei servizi di comunicazione sulla decadenza del termine, per cui, un dato che doveva essere cancellato, è stato invece trasmesso. In aggiunta questa illegittimità rappresenta un enorme problema per la tenuta delle indagini, le quali corrono il rischio di essere così travolte con conseguenze negative per il proseguo delle stesse, tenuto conto anche dell'importanza investigativa dei dati esterni alle comunicazioni. Un'indagine che si dimostra solida sin da subito, si esporrebbe al rischio di non convertirsi in una fondata azione penale e di non confluire, in seguito, in uno stabile procedimento.

In conclusione, la disciplina introdotta dal d. lgs. 10 agosto 2018 n. 101, presenta delle criticità anche in riferimento al rapporto tra le differenti tempistiche per la conservazione dei dati e in relazione al principio di ragionevole durata del processo. Queste problematiche, che risultano tutt'ora in discussione, verranno trattate nel corso dell'elaborato.

2. 2 La sentenza della Corte di Giustizia dell'Unione Europea C- 746/18, del 2 marzo 2021

Una pronuncia importante a livello europeo, che ha nuovamente influito sullo sviluppo di una disciplina completa della "*data retention*", è stata la sentenza della Corte di Giustizia, Grande Sezione, C-746/18 pronunciata il 2 marzo 2021. Questa

sentenza ha riassunto principi già trattati[88] ma si è soffermata su aspetti fino a questo momento mai esaminati.

La questione riguardava una decisione del Tribunale di primo grado di Viru, Estonia, sulla condanna della signora H.K. ad una pena detentiva di due anni di reclusione per aver commesso una serie di furti, per l'utilizzo di una carta bancaria di un terzo soggetto e per episodi di violenza nei confronti di soggetti partecipanti ad un procedimento. Il Tribunale, al fine di pronunciarsi sulla condanna, si è basato su "vari processi verbali"[89] redatti sulla base di dati[90] di comunicazioni elettroniche, raccolti, dall'autorità incaricata dell'indagine, dai fornitori dei servizi di comunicazione.

La signora H.K. presenta ricorso in Cassazione avverso questa decisione, nel quale contesta l'ammissibilità dei suddetti processi verbali in quanto risulterebbe che la legge estone sulle comunicazioni elettroniche, con i relativi obblighi per i fornitori dei servizi, sia contraria all'art. 15 della Direttiva 2002/58/CE e agli articoli 7, 8, 11 e 52[91] della Carta dei Diritti Fondamentali dell'Unione Europea.

Il giudice estone ritiene che il punto centrale del ricorso sia stabilire se l'art. 15 della Direttiva, letto alla luce degli articoli sopra citati previsti dalla Carta, debba essere interpretato in un'ottica di consentire alle autorità nazionali l'accesso ai dati per identificare la fonte e la destinazione di una comunicazione, ma solo in casi di criminalità grave, in quanto viene visto come un'ingerenza nei diritti fondamentali dell'individuo. Inoltre il giudice manifesta delle perplessità in relazione alla figura, e nello specifico all'indipendenza, del Pubblico Ministero estone come autorità che possa autorizzare l'accesso a queste forme di conservazione dei dati. Alla luce di

[88] Principi già affermati in Corte giust. UE, 8 aprile 2014, *Digital Rights Ireland* e Corte giust. UE, 21 dicembre 2016, *Tele2 e Watson*.
[89] Punto 17, Corte giust. UE, *H.K. v. Prokuratuur*, C-746/18.
[90] Si parla di dati relativi ai numeri di telefono di H.K. e diversi codici internazionali di identificazione di dispositivi di telefonia mobile.
[91] Rispettivamente: art. 7 (rispetto della vita privata e della vita familiare); art. 8 (protezione dei dati di carattere personale); art. 11 (libertà di espressione e di informazione); art. 52 (portata ed interpretazione dei diritti e dei principi).

quanto detto, il giudice estone decide di sospendere il procedimento interno e rinviare pregiudizialmente alla Corte di Giustizia.

Nello specifico, vengono sottoposte alla Corte tre questioni: la prima concerne l'ingerenza nei diritti fondamentali causata dall'accesso ai dati da parte dell'autorità, al fine di decidere se limitare questa forma di accesso ai soli reati gravi; la seconda questione riguarda il principio di proporzionalità e la sua applicazione con riferimento alla quantità di dati cui le autorità nazionali hanno accesso e la gravità dei reati perseguiti tramite questa ingerenza; la terza questione si riferisce alla possibilità di subordinare l'accesso ai dati, da parte dell'autorità, ad un controllo preventivo effettuato o da un giudice o da un'autorità amministrativa indipendente con attenzione sulla figura del Pubblico Ministero estone.

La Corte tratta congiuntamente le prime due questioni e dichiara che l'art. 15 della Direttiva 2002/58/CE, esaminato in sinergia con gli articoli 7, 8, 11, e 52 della Carta, contrasta con una normativa nazionale, la quale preveda l'accesso da parte di pubbliche autorità ai dati relativi al traffico, idonei a fornire informazioni sulle comunicazioni effettuate da un soggetto utente, per finalità di prevenzione, accertamento e perseguimento di reati, senza che tale accesso sia circoscritto a gravi forme di criminalità indipendentemente dalla durata del periodo per il quale l'accesso ai suddetti dati viene richiesto, nonché dalla quantità o dalla natura dei dati disponibili per tale periodo. Di conseguenza la Corte afferma che il potere di acquisizione delle tipologie di dati, previsti dalla disciplina della "*data retention*", venga limitato e circoscritto all'attività di repressione ed accertamento di gravi reati o di gravi minacce per la sicurezza nazionale.

Invece, in relazione alla terza questione, i giudici della Corte affermano come sia essenziale e importante che la procedura di accesso e di acquisizione dei dati, da parte della pubblica autorità, venga subordinata ad un controllo preventivo effettuato da un giudice o da un'autorità amministrativa indipendente. La decisone di tale giudice o di tale autorità perverrà a seguito di una richiesta formale presentata

dall'autorità pubblica che gestisce le indagini. La Corte, inoltre, individua anche quelli che sono i requisiti che l'autorità di controllo deve possedere: in particolare si fa riferimento al requisito della terzietà rispetto all'autorità che svolge le indagini e che richiede l'accesso ai dati e la loro acquisizione, affinché il controllo venga svolto in "modo obiettivo e imparziale al riparo da qualsiasi influenza esterna"[92]. Con specifico riferimento all'ambito penale, la Corte afferma che il requisito, così delineato, dell'indipendenza implica che l'autorità responsabile del controllo non debba essere coinvolta nella conduzione delle indagini e debba rivestire una posizione di neutralità nei riguardi delle parti del procedimento. Si conclude quindi l'esame della terza questione affermando che l'art. 15 della Direttiva 2002/58/CE, insieme agli articoli 7, 8, 11, 52 della Carta, "deve essere interpretato nel senso che esso osta ad una normativa nazionale, la quale renda il Pubblico Ministero, il cui compito è di dirigere il procedimento istruttorio penale e di esercitare, eventualmente, l'azione penale in un successivo procedimento, competente ad autorizzare l'accesso di un'autorità pubblica ai dati relativi al traffico e ai dati relativi all'ubicazione ai fini di un'istruttoria penale"[93].

In conclusione, la Corte di Giustizia, nel corso della motivazione, consolida la gravità dell'ingerenza nella sfera privata derivante dall'accesso ai dati di traffico da parte dell'autorità pubblica e ne ricava le dovute garanzie sia con riferimento allo scopo investigativo subordinato all'ingerenza, sia in relazione all'organo deputato e competente ad autorizzare l'accesso e l'acquisizione di tali dati. All'indomani di questa pronuncia, che viene definita "dirompente"[94], si era sviluppata l'idea per cui i principi delineati dalla sentenza stessa non dovessero riguardare gli Stati dotati di una regolamentazione in materia di accesso e di acquisizione dei dati, ma solo quegli Stati che erano privi di una disciplina in questione. Per cui la legislazione

[92] Punto 54, Corte giust. UE, 2 marzo 2021, *H.K. v. Prokuratuur* C-746/18.
[93] Punto 59, Corte giust. UE, 2 marzo 2021, *H.K. v. Prokuratuur* C-746/18.
[94] Così A. MALACARNE-G. TESSITORE, *La ricostruzione della normativa in tema di* data retention *e l'ennesima scossa della Corte di giustizia: ancora inadeguata la disciplina interna?*, in *A. Pen.,* 2022, p. 19. E anche N. SCERBO, *L'importanza dei dati e la loro gestione da parte dell'autorità*, in *Altalex*, 2023, p. 2 e ss.

italiana era ritenuta, all'inizio, adeguata a quando stabilito dalla Corte in quanto dotata di una normativa specifica in materia di *"data retention*".

Il problema era dato dal fatto che la Corte, nella completezza della sua motivazione, afferma che "la conservazione di tutti i metadati rappresenta una ingerenza particolarmente significativa nei diritti garantiti dalla Carta dei diritti fondamentali dell'Unione Europea, in quanto consente di accedere ad informazioni fondamentali della vita personale dei soggetti nei confronti dei quali vengono raccolti"[95].

Questa decisione è stata definita anche come "soluzione tampone"[96] avente lo scopo di individuare, e successivamente garantire, una giusta forma di equilibrio tra, da un lato, le esigenze di repressione di gravi forme di criminalità e, dall'altro, i diritti fondamentali della *privacy*, del rispetto della vita privata degli individui e della protezione dei dati personali. Questa definizione riflette l'instabilità e l'incompletezza della materia, entrambe sollevate anche nel corso di questo elaborato, ed è perciò opinione prevalente che un intervento a livello normativo interno e a livello giurisprudenziale europeo sia necessario.

Un passaggio ancora dubbio[97] attiene al profilo della doppia pregiudizialità di questioni, in caso di conflitti della normativa interna sia con principi e valori costituzionali sia con i medesimi contenuti nella Carta. In particolare, non si rinviene nella motivazione della Corte una regola di applicazione diretta in riferimento ai principi contenuti nella Carta, tenendo anche conto dell'impostazione della Corte Costituzionale[98], la quale rivendica la supremazia e il primato del

[95] A. MALACARNE-G. TESSITORE, *La ricostruzione della normativa in tema di* data retention *e l'ennesima scossa della Corte di giustizia: ancora inadeguata la disciplina interna?*, in *A. pen.,* 2022, p. 20.
[96] J. DALLA TORRE, *L'acquisizione dei tabulati telefonici nel processo penale dopo la sentenza della Grande Camera della Corte di Giustizia UE: la svolta garantista in un primo provvedimento del g.i.p. di Roma,* in *Sistema Penale*, 2021, p. 4.
[97] N. SCERBO, *L'importanza dei dati e la loro gestione da parte dell'autorità*, in *Altalex*, 2023, p. 3 e ss.
[98] Esaminata da G. SCACCIA, *Corte costituzionale e doppia pregiudizialità: la priorità del giudizio incidentale oltre la Carta dei diritti?,* in *Quad. cost.,* 2020. In questo elaborato, l'autore fa riferimento alla sentenza della Corte Costituzionale n. 269 del 2017, con la quale la Corte stessa ha rivendicato la priorità del giudizio costituzionale rispetto al rinvio alla Corte di giustizia.

giudizio costituzionale rispetto al giudizio della Corte di Giustizia. Una soluzione che, alcuni autori prospettano[99], è quella di riconoscere un principio di diritto previsto dalla Corte in riferimento e alla luce dei principi stabiliti dalla Direttiva 2002/58/CE, eliminando ogni riferimento alla Carta, per facilitare il lavoro del giudice, il quale sarà così vincolato a quanto previsto dalla Direttiva a cui la motivazione della Corta rimanda, senza necessario intervento di controllo della Corte Costituzionale.

Questa pronuncia ha riacceso il dibattito in merito alla normativa interna della "*data retention*", interrogandosi sul come il legislatore italiano sarebbe intervenuto e se avrebbe condiviso o meno le argomentazioni della Corte.

2. 3 Il d. lgs. 30 settembre 2021, n. 132 e la questione di illegittimità costituzionale

A seguito della sentenza della Corte di Giustizia sul caso H.K., le Corti dei vari paesi europei si sono interrogati sulla conformità della loro disciplina in materia di "*data retention*". In particolare, il Governo Italiano ha deciso di intervenire sulla disciplina interna della conservazione ed acquisizione dei metadati, ammettendo che la suddetta disciplina necessitasse di una modifica anche alla luce del nuovo dettato giurisprudenziale europeo, come già ammesso dal Governo stesso in occasione dell'esame del disegno di Legge europea del biennio 2019/2020[100],

Anche la Cassazione italiana si è pronunciata[101], all'indomani della sentenza H.K., affermando che l'interpretazione fornita dalla Corte di Giustizia sia del tutto

[99] Tra questi N. SCERBO, *L'importanza dei dati e la loro gestione da parte dell'autorità*, in *Altalex*, 2023, p. 2 e ss.
[100] Nell'Ordine del Giorno accolto dall'Italia erano presenti delle considerazioni in riferimento alla disciplina della "*data retention*", con particolare attenzione ai rischi legati all'accesso e all'acquisizione dei dati per i diritti fondamentali.
[101] Cass., Sez. II, 15 aprile 2021, n. 28523.

generica in riferimento all'individuazione di quelli che sono i casi che giustificano l'acquisizione dei dati di traffico telefonico e telematico e in più ritiene come sia necessario intervenire a livello normativo per disciplinare una materia così delicata, poiché vi è il rischio che venga regolata da singole pronunce giurisprudenziali anche disomogenee tra loro.

Sulla base di queste indicazioni, e vista l'urgenza[102], il Governo ha emanato il d. lgs. 30 settembre 2021, n. 132[103]. Questa norma non è integralmente dedicata alla disciplina della "*data retention*", in quanto regolamenta aspetti molto diversi fra loro, perciò solo l'art. 1 del presente decreto riporta delle modifiche alla normativa in materia di acquisizione dei dati, modificando l'art. 132 codice *privacy*.

Questo decreto ha introdotto due novità procedurali. *In primis* la figura del giudice viene investita del delicato compito del controllo preventivo all'acquisizione, il quale deve terminare con un decreto motivato che autorizzi o meno l'acquisizione stessa e che viene attivato con la presentazione da parte del Pubblico Ministero o del difensore dell'imputato, della persona sottoposta alle indagini[104], della persona offesa e delle altre parti private, di una richiesta formale. *In secundis* hanno circoscritto la possibilità di avviare la procedura di acquisizione dei dati ai soli casi in cui l'attività di indagine fosse finalizzata all'accertamento e repressione di reati definiti, per la prima volta, "gravi". Nello specifico la norma afferma che le parti legittimate possano presentare la richiesta di acquisizione dei dati in caso di sussistenza di "sufficienti indizi di reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, determinata

[102] Anche il Garante per la protezione dei dati personali, Pasquale Stanzione, ha più volte affermato che una riforma in materia era necessaria e, in molte occasioni, ha rimarcato le sue perplessità in relazione alla disciplina della "*data retention*" e del suo coordinamento con la lg. 167/2017. Ecco che il Governo italiano ha così giustificato la tipologia di atto adottato e le condizioni di necessità ed urgenza ex art. 77 Cost.

[103] Denominato Misure urgenti in materia di giustizia e difesa, nonché proroghe in tema di *referendum*, assegno temporaneo e IRAP, pubblicato in Gazzetta Ufficiale il 30 settembre 2021.

[104] È necessario ribadire che con la riforma è stato eliminato il precedente riferimento all'accesso diretto, da parte del difensore dell'imputato o dell'indagato, ai dati delle chiamate in entrata. A seguito del d. lgs. 30 settembre 2021, n. 132, il difensore dell'imputato o dell'indagato è tenuto a presentare istanza per l'acquisizione dei dati al giudice.

a norma dell'art. 4 c.p.p., 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, ove rilevanti ai fini della prosecuzione delle indagini, …"[105]. Questa modifica è stata predisposta, secondo parte della dottrina[106], a seguito di un'ordinanza del G.i.p del Tribunale di Roma, nella quale si affermava di utilizzare la procedura prevista per le intercettazioni anche nel caso di acquisizione di dati di traffico telefonico o telematico, al fine di rispettare *in toto* quanto espresso dalla Corte di Giustizia nella pronuncia del 2 marzo 2021, sul caso H.K. Di conseguenza, il legislatore è intervenuto individuando però un limite edittale inferiore rispetto a quanto indicato nelle norme che regolano la disciplina delle intercettazioni.

In più la riforma ha aggiunto un ulteriore comma, il comma 3-*bis*. Questo comma prevede una procedura di urgenza a carattere eccezionale, secondo la quale viene attribuita la possibilità, direttamente al Pubblico Ministero, di procedere con l'acquisizione dei dati, qualora vi sia un fondato motivo di possibile pregiudizio per la tenuta e la genuinità delle indagini derivante dal ritardo dato dalla procedura ordinaria. Questa procedura è sì eccezionale e rapida, ma necessita di una successiva convalida da parte del giudice entro quarantotto ore dalla comunicazione fornita dal Pubblico Ministero. Se questa procedura d'urgenza non dovesse ripercorrere i passaggi stabiliti dalla norma, i dati acquisiti saranno inutilizzabili.

Si ritiene, dunque, che queste modifiche siano in linea con quanto affermato dalla Corte di Giustizia nella sentenza H.K. In particolare si nota come il Governo si sia concentrato maggiormente nella creazione di una procedura più giurisdizionalizzata prevedendo, in aggiunta, l'introduzione dell'innovativo presupposto della gravità del reato.

[105] Art. 1 d. lgs. 30 settembre 2021, n. 132.
[106] M. BORGOBELLO, *Acquisizione di tabulati telefonici: che cosa cambia col nuovo decreto-legge*, in *Agenda Digitale*, 2021, p. 3 e ss.

Sul fronte delle critiche, è opportuno esaminare per prima una questione molto importante sollevata dalla dottrina e che destabilizza l'intera riforma.

Dal punto di vista metodologico, il problema che viene sollevato riguarda la possibilità che il decreto sia affetto da vizio di legittimità costituzionale per mancanza del requisito di omogeneità delle disposizioni in esso contenute. Già dall'esame della intitolazione del decreto, si evince come, al suo interno, vengano trattati aspetti molto differenti tra loro e che non riguardino solo la disciplina della "*data retention*". Inizialmente la giurisprudenza costituzionale aveva consolidato come principio quello che giustificava l'esercizio da parte del Governo delle potestà legislative previste all'art. 77 della Costituzione, tramite l'emanazione di decreti legge dotati di "intrinseca coerenza delle norme contenute, o dal punto di vista oggettivo e materiale, o dal punto di vista funzionale e finalistico"[107]. Perciò la Corte richiedeva che il decreto rispettasse, con riferimento al suo contenuto, questo criterio di omogeneità, in quanto la realizzazione di un provvedimento d'urgenza che contenesse norme disomogenee tra loro, renderebbe il decreto uno strumento per approvare norme accomunate solo da causalità temporale. È evidente come, nel caso del decreto in esame, venga meno il requisito della omogeneità tra le questioni trattate, sostituito da una chiara disomogeneità.

Ma successivamente, la Corte Costituzionale ha leggermente modificato la sua impostazione dando per salvi i decreti legge che disciplinino ambiti materiali diversi, con l'unica raccomandazione che suddetti decreti puntino ad un unico scopo, ovvero quello di intervenire in breve tempo su questioni ritenute rilevanti ed importanti dal Governo e dal Parlamento. Per cui l'omogeneità di scopo viene ritenuta dalla Corte sufficiente per giustificare un provvedimento governativo a contenuto differenziato ed eterogeneo. Nemmeno l'omogeneità di scopo è facilmente individuabile nel decreto in esame.

[107] Corte Cost., sentenza n. 22 del 16 febbraio 2012.

Sulla base di queste considerazioni, secondo parte della dottrina[108] sarebbe stato opportuno sollevare questione di illegittimità costituzionale a fronte della disomogeneità non solo di contenuti, ma anche di scopo. Inoltre, è parere condiviso dalla stessa dottrina[109] che, soprattutto la delicata disciplina della "*data retention*", avrebbe dovuto essere regolata ricorrendo ad una legge ordinaria, sottoponendo tutte le relative questioni al dibattito parlamentare.

In relazione alle molteplici criticità, anche l'associazione nazionale Magistrati[110] si è esposta criticando duramente la scelta del governo, ritenuta eccessivamente garantista con effetto paralizzante degli uffici e delle cancellerie di Procure e Tribunali. La critica di fondo richiama la mancata tutela effettiva della *privacy* con maggiore burocrazia per gli uffici, nonostante venga più volte richiamata l'importanza investigativa dell'acquisizione dei dati di traffico telefonico e telematico, in quanto strumento poco invasivo e indispensabile nelle prime fasi delle indagini preliminari.

2. 4 Ulteriori criticità del d. lgs. 30 settembre 2021, n. 132: la mancata predisposizione di un limite soggettivo all'acquisizione dei dati, il profilo della determinazione dei reati presupposto e il problema della figura del Pubblico Ministero

È necessario analizzare le ulteriori criticità sollevate da gran parte degli esperti del diritto processuale penale. Una prima criticità concerne la mancata previsione di un

[108] In particolare da Giacomo Pestelli, sostituto procuratore presso la Procura della Repubblica di Firenze nel suo scritto, *D. L. 132/2021: un discutibile e inutile aggravio di procedura per tabulati telefonici e telematici*, in *Altalex*, ottobre 2021, p. 3 e ss.

[109] Sempre Giacomo Pestelli, sostituto procuratore presso la Procura della Repubblica di Firenze.

[110] P. FROSINA*, La nuova legge sui tabulati telefonici non tutela la privacy ma rallenta inchieste e processi. E su alcuni reati sarà più difficile indagare*, in *Il Fatto Quotidiano*, 2021. L'associazione si è espressa nella persona del sostituto procuratore della Direzione distrettuale antimafia di Reggio Calabria, il Dott.re Stefano Musolino, il quale ha sottolineato come la normativa così delineata dal governo causerà: da un lato indagini e procedimenti più lenti, dall'altro, impossibilità di indagare per alcune tipologie di reati non comprese nei termini edittali previsti dalla norma.

limite soggettivo all'acquisizione dei dati, il quale avrebbe così individuato una categoria di soggetti nei confronti dei quali fosse consentito l'accesso ai dati[111].

La dottrina si è divisa in relazione a questa previsione. Alcuni esperti[112] ritengono che sia necessario individuare i soggetti in base al loro coinvolgimento nella fattispecie criminosa per la quale si procede. Nello specifico, si richiama a quanto previsto dalla Corte di Giustizia nella sentenza H.K., secondo la quale l'accesso è consentito soltanto in relazione ai dati di soggetti sospettati di aver commesso o di poter commettere un illecito grave contro la sicurezza nazionale. Sulla base di questa interpretazione richiamata da parte della dottrina, era indispensabile indicare i soggetti sospettati nei confronti dei quali si potesse procedere con l'acquisizione dei dati e i soggetti non sospettati contro i quali, solo in situazioni particolari, si concedesse l'autorizzazione a procedere all'acquisizione dei dati, ma a condizione che esistano "elementi oggettivi che permettano di ritenere che tali dati potrebbero, in un caso concreto, fornire un contributo effettivo alla lotta contro attività di questo tipo"[113].

L'altra parte della dottrina[114], invece, sostiene l'idea opposta. Ritengono l'impostazione presentata dalla Corte di Giustizia restrittiva dei soggetti destinatari dell'operazione di acquisizione dei dati. Secondo questa scuola di pensiero, un'elencazione chiusa dei soggetti passivi all'acquisizione dei dati evidenzierebbe "l'inadeguatezza rispetto alle molteplici situazioni che si potrebbero concretamente manifestare nella prassi"[115].

---

[111] Sul punto anche la sentenza della Corte giust. UE , 2 marzo 2021, *H.K. v. Prokuratuur* C-746/18, aveva specificato che fossero necessari dei criteri che stabilissero le circostanze e le condizioni che permettessero alle autorità nazionali di procedere all'acquisizione dei dati relativi ad un soggetto.

[112] In particolare Leonardo Filippi, avvocato e professore ordinario di diritto processuale penale all'Università degli studi di Cagliari.

[113] L. FILIPPI, *La nuova disciplina dei tabulati: il commento "a caldo" del Prof. Filippi*, in *Penale. Diritto e procedura*, 2021, p. 11.

[114] Rappresentata da Alessandro Malacarne, dottorando di ricerca in diritto processuale penale presso l'Università degli studi di Genova.

[115] A. MALACARNE, *La decretazione d'urgenza del Governo in materia di tabulati telefonici: breve commento a prima lettura del d. l. 30 settembre 2021, n. 132*, in *Sistema Penale*, 2021, p. 11.

La linea scelta dal Governo di non seguire quanto previsto dalla Corte, non solo non impedisce l'acquisizione dei dati degli imputati e degli indagati, ma inoltre consente di procedere all'acquisizione nei procedimenti contro ignoti o nei confronti di soggetti che anche inavvertitamente abbiano fatto parte dell'*iter* criminoso o siano semplicemente coinvolti in qualità di persona offesa o di testimone. A parere di chi scrive, si ritiene che la soluzione appena prospettata sia la più adatta anche a fronte di un irrigidimento della procedura con l'introduzione del controllo preventivo in capo al giudice.

Un ulteriore profilo che ha destato delle preoccupazioni riguarda la determinazione dei reati presupposto per l'espletamento della procedura di acquisizione. Secondo alcuni[116] la disposizione dei presupposti, così come delineati all'art. 1 del d. lgs. 30 settembre 2021 n. 132, ha comportato una selezione molto scarsa dei reati legittimanti l'acquisizione, visto che i suddetti criteri "finiscono di fatto col comprendere fattispecie che paiono carenti di una reale gravità"[117].

Per l'altra parte della dottrina[118] questa impostazione impedisce di perseguire dei reati che, seppure non superino quel livello di gravità previsto dal d. lgs. 30 settembre 2021 n. 132, comunque corrispondo a fattispecie meritevoli di sanzione. Di conseguenza con riferimento a tutte le fattispecie non punite con la pena dell'ergastolo o con una pena inferiore ai tre anni di reclusione, l'autorità che indaga non potrà avvalersi, in ambito investigativo, dello strumento della "*data retention*" con conseguenze negative sia per le indagini in senso stretto, sia per le vittime e i loro diritti. Per esempio, si fa riferimento ai reati come la sostituzione di persona di cui all'art. 494 c.p., alla turbata libertà dell'industria o del commercio previsto

[116] Tra i quali Giuseppe Amato, prima procuratore capo della procura di Bologna e attualmente Procuratore Generale a Roma, e anche Federica Rinaldini, avvocato penalista.
[117] G. AMATO*, Nella "costruzione" normativa si è sminuito il ruolo del Pm*, in *Guida al diritto*, 2021, p. 22.
[118] Rappresentata da Giacomo Pestelli, attualmente sostituto procuratore presso la Procura di Firenze. Nel suo scritto, *D. L. 132/2021: un discutibile e inutile aggravio di procedura per tabulati telefonici e telematici*, in *Altalex*, ottobre 2021, p. 5, l'autore presenta un elenco specifico di tutte le fattispecie che restano escluse dalla disciplina in quanto non superano il criterio della gravità.

all'art. 513 c.p., alla rivelazione di segreti scientifici o commerciali o alla rivelazione colposa di segreti d'ufficio rispettivamente disciplinati agli artt. 623 e 326, comma 2 c.p.

È opportuno concentrarsi anche sulla terminologia delle parole utilizzate nella definizione di reato grave, dove è possibile individuare delle discrepanze con i reati che rientrano nella suddetta definizione. In particolare, il concetto di "minaccia grave" è rinvenibile nella lettura di alcune disposizioni normative, come ad esempio nell'art. 339 c.p. e nell'art. 612 comma 2 c.p., mentre i concetti, sempre introdotti dal decreto, di "molestia" e "disturbo gravi" non sono individuabili nelle norme esistenti. Questi concetti sono del tutto nuovi e quindi possono essere assoggettati a numerose e differenti interpretazioni, causando una profonda incertezza e imprevedibilità delle decisioni.

Per ultimo, si esamina il profilo della diretta applicabilità della decisione della Corte di Giustizia. La giurisprudenza italiana di merito si era divisa[119] sulla diretta applicabilità della stessa nel nostro ordinamento, mentre, come abbiamo già visto, la Cassazione ne aveva escluso la diretta applicabilità[120], auspicando un intervento del legislatore. Anche la dottrina[121] aveva manifestato, nel suo pensiero prevalente, il contrasto alla diretta applicabilità della sentenza della Corte di Giustizia, facendo leva sulla regola stabilita dall'art. 267 T. F. U. E., secondo la quale le pronunce della Corte di Giustizia non sono immediatamente applicabili e operanti

[119] Il tribunale di Roma, tramite il decreto 25 aprile 2021, Sez. G.i.p., riteneva direttamente applicabile la sentenza della Corte di Giustizia con effetti vincolanti *erga omnes* rilevando il contrasto tra l'art. 132 codice *privacy* e l'art. 15 della Direttiva 2002/58/CE.

[120] Affiancata anche dalla Corte d'Assise di Napoli e dal tribunale di Tivoli che escludevano la diretta applicabilità della sentenza della Corte di Giustizia a causa della eccessiva indeterminatezza.

[121] F. VECCHIO, *L'ingloriosa fine della direttiva* Data retention*, la ritrovata vocazione costituzionale della Corte di Giustizia e il destino dell'art. 132 del Codice della* privacy, in *Rivista elettronica del Centro di Documentazione Europea dell'Università Kore di Enna*, 2014. E anche C. PARODI, *Tabulati telefonici: la Suprema Corte si esprime dopo le indicazioni della CGUE*, in *Il penalista.it*, 2021.

nell'ordinamento interno degli Stati Membri, in quanto esse incidono solo nei riguardi degli atti interni dell'Unione[122].

Nella predisposizione del procedimento di acquisizione, così come stabilito all'indomani del d. lgs. 30 settembre 2021 n. 132, il legislatore non ha tenuto conto di una divergenza fondamentale tra l'ordinamento italiano e l'ordinamento estone, oggetto del caso esaminato e deciso dalla Corte di Giustizia: la figura del Pubblico Ministero estone con le sue funzioni e i suoi compiti presenta solide differenze con la figura italiana del Pubblico Ministero. Nel nostro ordinamento, il Pubblico Ministero gode di tutta una serie di garanzie di autonomia e indipendenza dal Governo assicurate da alcune norme presenti in Costituzione[123], le quali non lo possono paragonare ad un'autorità amministrativa indipendente. Diversa è la qualifica della figura del Pubblico Ministero estone, il quale è un'autorità direttamente soggetta alla competenza e al controllo del Ministero della Giustizia. Controllo molto serrato, visto che il Ministro della Giustizia estone partecipa attivamente alla pianificazione del lavoro dei propri Pubblici Ministeri e all'individuazione delle misure di sorveglianza ritenute necessarie per la repressione dei reati sul territorio nazionale, rivestendo una posizione di superiore gerarchico dei Pubblici Ministeri.

In più, la disciplina italiana, precedente l'emanazione del decreto di cui si sta discutendo, prevedeva già la sussistenza di due entità distinte, la prima che richiedeva l'accesso ai dati e la seconda che lo autorizzava. Infatti, era previsto che fosse la polizia giudiziaria a chiedere l'accesso e l'acquisizione dei dati inerenti all'attività di indagine, mentre il Pubblico Ministero si occupava dell'eventuale rilascio dell'autorizzazione. Pertanto la terzietà e l'indipendenza dell'autorità deputata al controllo preventivo, alle quali la Corte di Giustizia fa riferimento nella motivazione della pronuncia H.K e ritenute da lei stessa come requisiti

[122] L. FILIPPI, *La Grande Camera della Corte di giustizia U.E. boccia la disciplina italiana sui tabulati*, in *Penale Diritto e Procedura*, 2021, p. 13.
[123] Si fa riferimento agli artt. 101, 102, 104, 105, 106, 107 e 108 Cost.

fondamentali della procedura di richiesta ed acquisizione dei dati, erano già presenti nella precedente normativa. Una parte della dottrina[124], minoritaria però, ha sollevato dei dubbi in relazione alla sussistenza del requisito della terzietà del Pubblico Ministero, in quanto la pubblica accusa è parte processuale e quindi coinvolta sin da subito nella vicenda con, ovviamente, interessi opposti alla difesa. Questa impostazione viene superata dalla convinzione, sostenuta dall'altra parte della dottrina[125], maggioritaria appunto, secondo la quale il Pubblico Ministero italiano soddisfi entrambi i requisiti di indipendenza e terzietà[126] stabiliti dalla Corte di Giustizia nella sentenza H.K.

Si ritiene quindi che le affermazioni della Corte di Giustizia non considerino il caso estone nella sua unicità e specificità e di conseguenza propongano una motivazione troppo generalizzata nei confronti di tutte le autorità inquirenti dei vari Stati, le quali sono dotate di regole e funzioni diverse. Gli esperti ritengono che questa questione vada rivista.

In conclusione, la scelta del Governo di ricorrere allo strumento del decreto legge, per tutte le ragioni sopra riportate, ha rappresentato un importante profilo di perplessità e criticità, sia in riferimento alle modalità sia in relazione ai risultati che si intendeva raggiungere. L'auspicio dell'epoca era quello che il Parlamento, in sede di conversione, ravvisasse le suddette criticità ed intervenisse apportando le dovute modifiche, magari restituendo al Pubblico Ministero le sue funzioni originarie.

---

[124] M. VIGGIANO, *Navigazione in* Internet *e acquisizione occulta di dati personali*, in *Dir. inf. e inf.*, 2007. E ancora R. MIRANDA, *Gli obblighi del gestore: esigenze di* data protection *o di* data retention*?*, Mezzi di comunicazione e riservatezza, Jovene, 2008. E anche R. FLOR-S. MARCOLINI, *Dalla* data retention *alle indagini ad alto contenuto tecnologico: la tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato,* Giappichelli, 2022, p. 6.

[125] V. TONDI, *La disciplina italiana in materia di* data retention *a seguito della sentenza della Corte di giustizia UE*, in *Sistema Penale*, 2021. E ancora S, SCAGLIARINI, *La Corte di Giustizia bilancia diritto alla vita privata e lotta alla criminalità: alcuni pro e alcuni contra*, in *Dir. inf. e inf.*, 2014.

[126] Infatti all'art. 358 c.p.p. rubricato "attività di indagine del pubblico ministero" si fa riferimento alle attività di indagine necessarie svolte dal Pubblico Ministero. Viene inoltre specificato come questi accertamenti vegano eseguiti anche su fatti e circostanze a favore della persona sottoposta alle indagini.

2. 5 La conversione in legge del d. lgs. 30 settembre 2021, n. 132 e l'applicazione ai procedimenti in corso

La legge di conversione del decreto[127] ha apportato una serie di modifiche all'originaria formulazione, lasciando però inalterati alcuni profili problematici.

Dalla lettura delle modifiche apportate, si può notare come il legislatore sia intervenuto sul requisito della rilevanza dell'accesso e dell'acquisizione dei dati. Inizialmente il decreto prevedeva che l'acquisizione dei dati dovesse avvenire "ai fini della prosecuzione delle indagini[128]", espressione ritenuta troppo circoscritta e limitata. Il legislatore ha perciò previsto un'espressione più ampia, affermando che l'acquisizione dei dati fosse prevista "per l'accertamento dei fatti[129]". Di conseguenza, questa espressione consente di comprendere un ampio spettro di attività di indagine, sia con riferimento alle indagini del Pubblico Ministero sia a quelle difensive. Inoltre, questa scelta è idonea a proiettare l'applicazione della norma anche nelle altre fasi del procedimento e quindi oltre la fase delle indagini preliminari, ricomprendendo anche la fase processuale del dibattimento, e successivamente, anche il giudizio di appello.

In secondo luogo, il legislatore ha apportato un ulteriore modifica in merito alle modalità operative della procedura di acquisizione dei dati. Il precedente decreto aveva generato un dubbio in relazione alla alternativa se i tabulati dovessero essere acquisiti presso il fornitore del servizio per mezzo della notifica del provvedimento autorizzativo del giudice, oppure se il provvedimento del giudice dovesse essere seguito da un provvedimento specifico della parte richiedente, Pubblico Ministero o difensore, indirizzato direttamente al fornitore del servizio. Il rischio evidenziato dall'eventualità che l'acquisizione avvenisse solo ricorrendo al decreto motivato del giudice, era costituito da una possibile fuga di notizie riservate in quanto la fase delle indagini è coperta dal segreto istruttorio e il decreto stesso del giudice contiene

[127] Lg. di conversione 23 novembre 2021, n. 178
[128] D. lgs. 30 settembre 2021, n. 132.
[129] Nuova formulazione introdotta con la lg. di conversione 23 novembre 2021, n. 178.

i nominativi delle persone indagate e l'oggetto principale delle indagini, con il pericolo di rivelare, a soggetti non qualificati, importanti elementi investigativi.

Questo dubbio di natura operativa, che ha portato il legislatore ad intervenire in sede di conversione, era dato dal fatto che il decreto non prevedesse nulla in merito. Di conseguenza è stato specificato che "i dati sono acquisiti previa autorizzazione rilasciata dal giudice con decreto motivato, su richiesta del Pubblico Ministero o su istanza del difensore dell'imputato…"[130]. Da questa formulazione, è chiara la natura del provvedimento del giudice, ovvero un decreto di tipo autorizzatorio. Toccherà successivamente alla parte istante, Pubblico Ministero o difensore, procedere alla concretizzazione di quanto autorizzato dal giudice, con un'apposita richiesta indirizzata al fornitore del servizio[131].

Un aspetto che resta oscuro, in quanto non disciplinato nemmeno dalla legge di conversione, concerne le modalità pratiche con cui dar seguito a tutte le richieste e le autorizzazioni formali. Resta quindi non disciplinato e facilmente interpretabile, il *quomodo* dell'acquisizione in senso stretto, con specifico riferimento alla problematica sopra esaminata relativa alla notifica al fornitore del servizio del decreto autorizzativo del giudice nella sua integrità o solo in parte. L'opinione prevalente[132], al quale l'autrice si associa, è quello di ritenere che non sia necessario allegare alla richiesta, che la parte istante indirizza al fornitore del servizio, il decreto autorizzativo del giudice, reputando sufficiente indicare la sua esistenza negli atti del procedimento[133].

---

[130] Nuova formulazione della lg. di conversione 23 novembre 2021, n. 178.

[131] Opinione sostenuta anche da R. FLOR-S. MARCOLINI, *Dalla* data retention *alle indagini ad alto contenuto tecnologico: la tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato,* Giappichelli, 2022, p. 50 e anche da A. NATALINI, *Misure urgenti in tema di acquisizione dei dati relativi al traffico telefonico e telematico a fini di indagine penale (art. 1 d. l. 30 settembre 2021, n. 132)*, Ufficio del Massimario e del Ruolo, Servizio Penale, Rel. N. 55/2021, in M. ACIERNO-G. ANDREAZZA (a cura di), Roma, 13 ottobre 2021, p. 21.

[132] Presentata da G. PESTELLI in *Convertito in legge il D. L. 132/2021: le modifiche apportate (e quelle mancate) in materia di tabulati*, in *Altalex*, novembre 2021.

[133] Con relativa responsabilità del soggetto dichiarante in riferimento a quanto dichiarato.

Un terzo elemento di incertezza, nei confronti del quale la legge di conversione ha previsto dei chiarimenti, attiene il profilo della sanzione dell'inutilizzabilità dei dati acquisiti in violazione delle previsioni legislative. In precedenza, l'inutilizzabilità era prevista solo nel caso di mancata convalida da parte del giudice, in sede di procedura d'urgenza, del decreto emesso dal Pubblico Ministero. Gli esperti[134] si sono chiesti se questa sanzione potesse essere estesa anche nell'ipotesi di violazione delle regole in materia di presupposti per l'operatività della norma e di violazione della disciplina ordinaria di acquisizione. Il legislatore ha previsto così l'introduzione di un nuovo comma 3-*bis*, il quale stabilisce "il divieto di utilizzazione dei dati acquisiti in violazione delle nuove previsioni riguardanti sia la procedura autorizzatoria ordinaria da parte del giudice, sia quella di acquisizione in via d'urgenza da parte del Pubblico Ministero"[135]. Con questa modifica, il legislatore amplia la sanzione più pensate per gli elementi di prova a tutte le ipotesi di violazioni procedurali e sostanziali della norma.

Anche la legge di conversione ha suscitato nella dottrina una serie di critiche. La prima riguarda l'indifferenza mostrata dal legislatore in relazione ad una modifica, necessaria, del profilo delle tempistiche di conservazione dei dati da parte dei fornitori dei servizi. Il Parlamento ha deciso di concentrarsi esclusivamente su modifiche prettamente procedurali, senza però intervenire su un aspetto molto importante della disciplina della "*data retention*" che, ad oggi, causa ancora problematiche di non poca irrilevanza.

Una delle problematiche più considerevoli consiste nella disciplina transitoria inizialmente prevista[136] nel dettato originario del d. lgs. 30 settembre 2021 n. 132 e

---

[134] G. PESTELLI, *Convertito in legge il D. L. 132/2021: le modifiche apportate (e quelle mancate) in materia di tabulati*, in *Altalex*, novembre 2021 e G. FORMICI, *"*The three Ghosts of data retention*": passato, presente e futuro della disciplina italiana in materia di conservazione e acquisizione dei metadati per scopi investigativi. Commento a margine del d. l. 30 settembre 2021, n. 132 e relativa legge di conversione*, in *Osservatorio Costituzionale*, febbraio 2022.

[135] Così G. PESTELLI, *Converitito in legge il D. L. 132/2021: le modifiche apportate (e quelle mancate) in materia di tabulati*, in *Altalex*, novembre 2021, p. 3.

[136] La disposizione transitoria, inizialmente prevista, stabiliva l'acquisizione e l'utilizzabilità dei dati nei procedimenti pendenti all'entrata in vigore del decreto, ma solo nei casi di persistenza degli

successivamente eliminata prima della sua entrata in vigore, lasciando così ai singoli interpreti decisioni inerenti alla retroattività delle nuove disposizioni. Alcuni esperti[137] ritengono che l'eliminazione della disciplina transitoria sia una scelta da condividere, in quanto avrebbe creato "notevoli problemi in sede applicativa[138]", rappresentati da possibili ritardi che avrebbero colpito le procedure successive. Perciò, secondo questa interpretazione, i dati acquisiti nel rispetto della normativa previgente il d. lgs. 30 settembre 2021 n. 132 avrebbero dovuto essere considerati validi, legittimi e di conseguenza utilizzabili, in quanto vige il principio del *tempus regit actum*[139] escludendo così la retroattività della nuova normativa.

Altri commentatori[140], invece, auspicavano che fosse il legislatore stesso ad intervenire dando una disciplina transitoria al decreto, evitando che ogni giudice giungesse ad una decisione differente e disomogenea sulla utilizzabilità dei dati di traffico telefonico e telematico acquisiti nei procedimenti pendenti nell'intervallo temporale che comprende la data della pubblicazione della sentenza della Corte di Giustizia sul caso H.K.[141], fino al giorno precedente l'entrata in vigore del d. lgs. 30 settembre 2021, n. 132.

In riferimento a questa situazione, è intervenuto il legislatore in sede di conversione, introducendo definitivamente la disciplina transitoria, con modifiche al suo contenuto. Questa nuova disciplina transitoria prevede che i suddetti dati "possono essere utilizzati a carico dell'imputato solo unitamente ad altri elementi di prova ed

stessi presupposti sanciti dal decreto e sulla base di una valutazione effettuata successivamente dal giudice, come sorta di convalida del provvedimento emesso dal Pubblico Ministero. Ne parla anche M. BUFFA, "Data retention*" e diritto transitorio: un possibile punto fermo giurisprudenziale*, in *Quest. giust.*, 2022.

[137] Di questa opinione Giacomo Pestelli, già citato, e Claudio Gittardi, procuratore della Repubblica presso il Tribunale di Sondrio dal 2015.

[138] C. GITTARDI, *Sull'utilizzabilità dei dati del traffico telefonico e telematico acquisiti nell'ambito dei procedimenti pendenti alla data del 30 settembre 2021*, in *Giustizia Insieme*, ottobre 2021.

[139] Stabilito a livello giurisprudenziale dalla sentenza Cass., Sez. Un., 31 marzo 2011, n. 27919.

[140] Tra i quali, Federica Resta, avvocato e funzionaria del Garante per la protezione dei dati personali.

[141] Ovvero il 2 marzo 2021.

esclusivamente per l'accertamento dei reati[142]" che rientrano nella definizione di reato grave individuata nel d. lgs. 30 settembre 2021, n. 132.

Subito sono state sollevate numerose critiche, sia di merito che di metodo, alla disciplina in esame. La prima criticità si solleva in relazione alla forma della tecnica legislativa utilizzata. In particolare, si fa riferimento al fatto che questa modifica non è rinvenibile all'interno dell'art. 132 codice *privacy* in quanto è stata inserita solo all'interno del d. lgs. 30 settembre 2021 n. 132, comma 1-*bis*. Inutile affermare come questa scelta comporti più svantaggi che benefici e renda la disciplina di difficile coordinamento con quanto previsto dall'art. 132 codice *privacy*.

Un secondo aspetto che suscita perplessità è quello dell'inutilizzabilità prevista dalla norma solo come sanzione a carico della figura dell'imputato, senza citare espressamente anche la figura dell'indagato. Si ritiene che questa previsione si possa facilmente estendere anche all'indagato tramite un'estensione in *bonam partem* prevista all'art. 61 c.p.p.

Infine un ulteriore profilo, che non è stato esente da critiche, concerne la retroattività del requisito della gravità del reato, in quanto non è previsto nella disciplina transitoria. Le serie conseguenze che derivano da questa impostazione riguardano, *in primis* il rischio di travolgimento di interi atti di indagine legittimamente compiuti secondo le disposizioni vigenti in quel dato momento storico per mezzo di una disposizione che, retroattivamente ne sancisce l'inutilizzabilità, ed *in secundis* il travolgimento di tutte quelle attività investigative, riguardanti l'acquisizione di dati telefonici o telematici, in relazione alla repressione di reati che non rientrano nei limiti di gravità fissati dalla nuova normativa[143].

---

[142] D. lgs. 30 settembre 2021, n. 132, comma 1-*bis*.

[143] Anche la Corte di Cassazione è intervenuta in relazione alla disciplina transitoria così delineata. Nella sentenza n. 1054/2022 la Corte ha negato l'effetto retroattivo della norma introdotta con il d. lgs. 30 settembre 2021, n. 132. Inizialmente la Suprema Corte nel suo Massimario aveva già esaminato diverse soluzioni in merito. Nella motivazione della sentenza, la Cassazione ha ribadito la natura processuale della disciplina della "*data retention*", escludendo così ogni forma di retroattività.

Un quadro normativo così come delineato necessità sicuramente di un futuro intervento correttivo, anche da parte della Corte Costituzionale.

2. 6 La sentenza della Corte di Giustizia C-178/22 del 30 aprile 2024

Recentemente la Corte di Giustizia dell'Unione Europea si è espressa sulle disposizioni interne adottate in materia di "*data retention*", intervenendo nello specifico sul controllo preventivo del giudice e sul presupposto della gravità del reato.

Il caso, esaminato anche dalla Corte, riguarda due procedimenti penali a carico di ignoti per reati di furto aggravato[144] avvenuti ad ottobre e novembre 2021. Il Pubblico Ministero, nel corso delle indagini e al fine di procedere con l'identificazione degli autori dei suddetti reati, seguendo la normativa interna[145] ha chiesto al G.i.p, presso il Tribunale di Bolzano, il rilascio del decreto autorizzativo per l'acquisizione dei dati di traffico telefonico e di traffico telematico dei due telefoni oggetto del furto.

Il G.i.p solleva dei dubbi in relazione alla compatibilità della normativa interna nazionale con l'art. 15 della Direttiva 2002/58/CE, anche alla luce dell'interpretazione fornita dalla Corte stessa nella sentenza H. K. del 2 marzo 2021. I dubbi in questione vertono sulla soglia dei tre anni di reclusione, individuata dalla normativa italiana come pena minima per i reati gravi, necessaria quindi per poter richiedere al giudice l'autorizzazione all'acquisizione dei dati. Quindi, secondo l'impostazione del G.i.p, ricorrere alla procedura di acquisizione dei dati in questo caso aiuterebbe solo a perseguire reati "dotati di scarso allarme sociale e che sono

[144] Previsti agli artt. 624 e 625 c.p.p.
[145] Art. 132 codice *privacy*.

puniti solo a querela di parte[146]", in quanto furti e di modesto valore, causando inutilmente una grave ingerenza nella vita privata del soggetto.

In relazione a tali circostanze, il G.i.p presso il Tribunale di Bolzano ha deciso di sospendere il corso del procedimento e rinviare alla Corte la decisione in merito alla seguente questione pregiudiziale: è possibile individuare un contrasto tra l'art. 15 della Direttiva 2002/58/CE, letto anche in relazione agli artt. 7, 8, 11 e 52 della Carta dei Diritti Fondamentali dell'Unione Europea, e la normativa interna prevista all'art. 132 codice *privacy*?

La Corte si pronuncia, in primo luogo, sulla natura della ingerenza, ritenuta grave dal giudice del rinvio, nella vita privata degli individui a seguito di acquisizione di dati telefonici o telematici. La Corte ritiene che suddetta ingerenza è da qualificarsi come grave a meno che non si riferisca alla repressione e alla lotta contro reati gravi e gravi forme di criminalità. Non rileva, invece, la circostanza per la quale è richiesta l'acquisizione dei dati non del proprietario del telefono cellulare rubato, ma dei soggetti che hanno utilizzato il telefono dopo il furto[147].

Successivamente, la Corte si concentra sulla definizione di reato grave. Viene ribadita l'esclusiva competenza degli Stati membri in relazione alla normativa penale e alle norme di procedura penale. La critica che la Corte muove in relazione alla nozione di reato grave, così come stabilita nella normativa italiana all'art. 132 codice *privacy*, riguarda il possibile "snaturamento"[148] della nozione di reato grave e "per estensione, anche di grave criminalità[149]". La conseguenza che ne deriva, secondo l'impostazione della Corte, è l'esercizio di un'ingerenza grave nella vita privata di un individuo in relazione a reati che "manifestamente non sono gravi con

[146] Come si legge dal punto 21 della sentenza Corte giust. UE, 30 aprile 2024 C-178/22.
[147] È la stessa Direttiva 2002/58/CE che afferma come l'obbligo di garantire la riservatezza delle comunicazioni elettroniche e la loro riservatezza riguardi le comunicazioni effettuate dagli "utenti". All'art. 2 la Direttiva definisce "utente" come qualsiasi persona fisica che utilizzi un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata.
[148] La Corte usa proprio questo termine.
[149] Corte giust. UE, 30 aprile 2024, C-178/22.

riguardo alle condizioni sociali esistenti nello Stato membro interessato[150]". Quindi, la Corte auspica che, per verificare se questo snaturamento sia avvenuto o meno, il controllo preventivo del giudice rappresenta un elemento essenziale. Mediante il suddetto controllo, il giudice verificherà la possibilità o meno che l'accesso ai dati causi una grave ingerenza nella vita privata del soggetto.

In terzo luogo, la Corte si concentra sull'eccessiva ampiezza della definizione di reato grave. La Corte non è d'accordo con il pensiero del giudice del rinvio in quanto la definizione di reato grave, prevista dalla normativa interna, si basa interamente su un criterio oggettivo, ovvero la pena detentiva stabilita dalla stessa norma.

Il punto più importante della riflessione della Corte concerne la possibilità che il giudice, deputato al controllo preventivo, neghi o limiti l'accesso ai dati. Perciò nei casi in cui vi sia il rischio di un'ingerenza grave nella vita privata di un soggetto e quando risulta che il reato non costituisca effettivamente una forma di grave criminalità, il giudice deve poter rigettare la richiesta presentata o limitare l'acquisizione dei dati. A sostegno di questo ragionamento, la Corte ribadisce che la funzione dell'autorità, incaricata del suddetto controllo, deve essere quella di garantire un equilibrio tra le esigenze investigative e il diritto alla *privacy* e al rispetto della vita privata.

Concludendo, la Corte afferma che la disposizione nazionale, così impostata, non contrasta con la Direttiva 2002/58/CE. La procedura di acquisizione dei dati di traffico telefonico e telematico resta prevista all'art. 132 codice *privacy* con il relativo presupposto della gravità del reato perseguito. L'unica condizione che la Corte evidenzia è, appunto, la possibilità che il giudice, in sede di controllo preventivo, possa decidere di negare o limitare l'accesso richiesto se l'indagine

[150] Corte giust. UE, 30 aprile 2024, C-178/22.

riguarda l'accertamento di un reato manifestamente non grave, in relazione alle condizioni della società in quel dato luogo e in quel momento.

All'indomani di questa sentenza, le criticità vertono, a parere di chi scrive, almeno su tre questioni: la maggiore discrezionalità del giudice, la costante diminuzione dei poteri di indagine in capo al Pubblico Ministero, ed infine l'elevazione del diritto alla *privacy* a discapito del diritto delle vittime di ottenere giustizia.

In primo luogo, la sentenza afferma come sia necessario che il giudice valuti se l'acquisizione dei dati possa tramutarsi in una grave ingerenza per la vita privata del soggetto e successivamente se il reato per cui si proceda sia manifestamente grave, nonostante rientri nel limite edittale di gravità del reato stabilito dalla disciplina interna. Questa discrezionalità[151], demandata al giudice, opera grazie a riflessioni anche, e soprattutto, in ambito sociale, in quanto viene chiesto a tale giudice di svolgere una valutazione in relazione a reati ritenuti dalla norma gravi, ma che in quel dato momento storico e in quel dato territorio di competenza non abbiano una connotazione così grave da giustificare e sorreggere un provvedimento autorizzatorio di accesso e acquisizione dei dati. Sulla base di questa impostazione, il dubbio concerne la natura e le modalità della verifica in ambito sociale demandata al giudice, sulla quale vi è il rischio che possa influire la discrezionalità e le scelte personali del giudice stesso, mancando una regola e uno schema solido che possano guidarlo in quanto non esperto di sociologia e di mutamenti della società.

In relazione alla seconda criticità, l'interpretazione della Corte si inserisce all'interno di quella visione garantista che opera ormai da alcuni anni. Il Pubblico Ministero viene ulteriormente limitato nelle sue funzioni di coordinatore delle indagini. A seguito quindi dell'interpretazione fornita dalla Corte, vi è il rischio che il Pubblico Ministero, che poteva contare sulla previsione legislativa di una serie di reati, ritenuti appunto gravi, nei confronti dei quali era possibile procedere con la

[151] Accennata anche da D. ALBANESE, in *Dalla Corte di giustizia dell'Unione europea un'altra svolta garantista in materia di acquisizione dei tabulati telefonici*, in *Sistema Penale*, maggio 2024, p. 6.

richiesta di acquisizione dei tabulati, debba attendere un ulteriore controllo preventivo del giudice che attenga alla manifesta pericolosità sociale del reato per cui si procede, nonostante venga espressamente ritenuto grave dalla norma. La possibile conseguenza che ne deriva riguarda una ipotizzabile perdita di poteri di indagine e maggiori difficoltà nella costruzione di un solido quadro probatorio, vista anche l'importanza dell'acquisizione dei dati telefonici e telematici per scopi investigativi.

Infine, si nota dalla sentenza come la linea di pensiero della Corte si riferisca ad una elevazione costante del diritto alla *privacy*. A parere di chi scrive, questa costante elevazione con conseguente diminuzione dei poteri di indagine in un'ottica garantista, da un lato attribuisce la giusta importanza ad uno dei diritti fondamentali dell'individuo, ma dall'altro rischia di diminuire le possibilità per le vittime di ottenere giustizia. Giustizia che lo Stato italiano deve assicurare nei modi e nei tempi previsti dalla legge. Con questa impostazione è ipotizzabile che il Pubblico Ministero non disponga di elementi di prova per esercitare l'azione penale e sorreggere un ragionevole previsione di condanna[152] nei confronti di un reato grave ma non ritenuto tale dal giudice a seguito della sua verifica in ambito sociale, con conseguente impossibilità per la vittima di ottenere giustizia.

In conclusione, sarà interessante attendere come sia la dottrina che il legislatore recepiranno eventualmente questa impostazione continuando a procedere in ottica garantista o retrocedendo rispetto all'area delle tutele.

[152] Come stabilito dalla riforma Cartabia, d. lgs. 10 ottobre 2022, n. 150.

CAPITOLO 3

3. 1 Le tempistiche di conservazione e di acquisizione dei dati

Il d.lgs. 10 agosto 2018 n. 101[153] ha apportato significative modifiche alla disciplina prevista dall'art. 132 codice *privacy*. In particolare, è intervenuto sull'originaria formulazione dell'art. 132 del codice *privacy.*[154]

All'indomani del d.lgs. 10 agosto 2018 n. 101, la disciplina della *"data retention"* si presenta totalmente riformata. Inoltre, questa disciplina è stata ulteriormente modificata con la legge europea n. 167 del 2017, la quale stabilisce in settantadue mesi il termine di conservazione dei dati previsti all'art. 132 del codice *privacy* relativi all'accertamento dei reati di matrice terroristica e appartenenti ad un elenco previsto all'art. 407 c.p.p[155].

Queste modifiche sono state oggetto di numerose critiche. Analizziamole di seguito.

Con riferimento alla riformulazione della norma, si può iniziare con la diversificazione delle tempistiche di conservazione dei dati. Nello specifico, la suddivisione temporale dei ventiquattro mesi per i dati di traffico telefonico, dei dodici mesi per i dati del traffico telematico e infine dei trenta giorni per le chiamate senza risposta, risulterebbero scadenze contrastanti non solo con le tempistiche investigative, ma anche con riferimento ai tempi generici della giustizia italiana[156].

---

[153] Recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del reg. (UE) 2016/679 del Parlamento Europeo e del Consiglio, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46 CE. Tale regolamento è entrato in vigore il 19/09/2018.

[154] D. lgs 30 giugno 2003, n.196, recante il codice in materia di protezione dei dati personali.

[155] Si tratta di reati quali: art. 285 c.p. (devastazione, saccheggio e strage), art. 286 c.p. (guerra civile), art. 416 *bis* c.p. (associazione si tipo mafioso), art. 422 c.p. (strage), art. 291 *ter* c.p., limitatamente alle ipotesi aggravate previste alle lett. a), d) ed e) del comma 2, e art. 291 *quater* c.p., comma 4, del testo unico delle disposizioni legislative in materia doganale approvato con d.p.r. 23 gennaio 1973, n. 43.

[156] Da uno studio condotto dal *"Sole 24 ore"* in data 4 Gennaio 2023 si evince come, in Italia, gli appelli penali durano dieci volte tanto la media europea. Il primo grado di giudizio dura, in media,

Si può anche notare come le scelte temporali intraprese siano del tutto disequilibrate anche tenendo conto, ad oggi, dell'importanza delle comunicazioni telematiche rispetto a quelle meramente telefoniche[157]. Importanza che, inevitabilmente, non è stata presa in considerazione visto che il traffico telematico è soggetto ad una scadenza dimezzata rispetto ai dati del traffico telefonico. Secondo parte della dottrina[158], infatti, questa differenziazione temporale tra dati di traffico telefonico e dati di traffico telematico appare "anacronistica"[159], in quanto ad oggi le comunicazioni telematiche "hanno sopraffatto ormai da tempo"[160] le comunicazioni telefoniche.

Queste suddivisioni temporali non rilevano ai fini dell'accertamento di delitti consumati o tentati con finalità di terrorismo, per i quali il termine di conservazione, unico, è di settantadue mesi dalla comunicazione. Si riscontra così un ulteriore criticità relativa alla disposizione, data dal fatto che, il nuovo comma introdotto con la legge europea in aggiunta ai commi già previsti dall'art. 132 codice *privacy*, facciano riferimento, impropriamente, all'esistenza di un "doppio binario"[161] a seconda del tipo di reato perseguito con conseguenti tempi di conservazione diversificati. Per i reati contenuti nell'art. 407 c.p.p. e per quelli a matrice terroristica, i termini di conservazione sono quelli previsti dalla legge europea, e quindi corrispondono ai settantadue mesi; mentre con riferimento alle altre fattispecie criminose i termini di conservazione dei dati corrispondono con lo scaglionamento previsto dall'art. 132 codice *privacy*.

Dal punto di vista pratico, una delle problematiche più rilevanti riguarda la figura degli *Internet Service Provider*, ovvero i fornitori di comunicazione elettronica.

---

498 giorni, ovvero oltre tre volte la media dei paesi europei, mentre il giudizio di Cassazione si attesta a 237 giorni rispetto ai 120 giorni di media in Europa.

[157] Tema affrontato anche da F. BUCCI, in *Data retention: stato dell'arte e sviluppi recenti in Europa*, in *Ius Itinere*, 2020.

[158] Rappresentata dall'avvocato Francesca Bucci di cui sopra.

[159] Cit. F. BUCCI, in *Data retention: stato dell'arte e sviluppi recenti in Europa*, in *Ius Itinere*, 2020.

[160] Cit. F. BUCCI, in *Data retention: stato dell'arte e sviluppi recenti in Europa*, in *Ius Itinere*, 2020.

[161] S. 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*., 11/2018, p.156.

Questi, nell'esercizio della loro funzione, non sono in grado di prevedere se i dati verranno loro richiesti da parte dell'autorità giudiziaria e per quale tipologia di reato. Di conseguenza, la soluzione che pragmaticamente è stata individuata, prevede che i fornitori conservino tutti i dati per la massima durata, ovvero per settantadue mesi. Se invece, la richiesta, da parte dell'autorità giudiziaria, di trasmissione e successiva acquisizione dei dati arrivasse entro uno dei termini previsti dall'art. 132 codice *privacy* e non si trattasse di uno dei reati disciplinati dalla legge europea, allora si potrebbe dire che la conservazione sia in linea con quanto previsto dalla norma[162].

Le conseguenze pratiche ed economiche che ricadono sugli *Internet Service Provider* sono considerevoli, ricordando anche che i suddetti sono qualificabili come soggetti di diritto con obblighi e responsabilità[163]. Per comprendere tale fenomeno è opportuno fare riferimento ad alcuni dati ricavati da uno studio realizzato dal Governo olandese riportato dal Garante della Privacy italiano.[164] La conservazione dei dati con tempistiche molto dilatate nel tempo causa tutta una serie di problematiche economiche ai fornitori, i quali dovranno necessariamente investire cifre significative per garantire l'espletamento delle loro funzioni. In particolare, solo con riferimento ad un "periodo di conservazione compreso fra i 12 e i 24 mesi, i costi di investimento nel 2005 coincidevano con 15-20 milioni di euro"[165]. Immaginando, quindi, una conservazione di settantadue mesi, si può

---

[162] S. 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*., 11/2018, p.157.

[163] I criteri di imputazione della responsabilità civile e penale per gli *Internet Service Provider* sono stabiliti dal d. lgs. 70/2003. Nel 2017 l'Unione Europea ha sviluppato ulteriormente la disciplina con l'intento di responsabilizzare l'ISP anche oltre quanto previsto dal d.lgs 70/2003. Ed infatti, la Commissione Europea, con le nuove linee guida del settembre 2017, ha aggravato gli oneri a carico dell'ISP sotto vari profili, sancendo dal un lato il c.d. "*TAKE-DOWN",* ovvero l'intervento necessario da parte dei singoli stati membri di introdurre una regolamentazione dettagliata sul procedimento di rimozione dei contenuti illeciti; e dall'altro il c.d. "*STAY-DOWN*" che risponde all'esigenza di evitare la ricomparsa dei contenuti illeciti.

[164] Pubblicato sulla Newsletter del Garante per la protezione dei dati personali il 23 gennaio del 2005.

[165] Lo studio è stato affidato dal governo olandese alla società di ricerche KPMG, con sede anche in Italia, la quale si è concentrata su dati di traffico rilevati fino al 2003.

rilevare come le spese per i fornitori aumentino considerevolmente. Tenendo conto che queste risultanze sono oggetto di proiezioni statistiche, gli esperti ritengono che queste stime siano inferiori alla realtà oggettiva.

Per di più, i fornitori sono anche responsabili della conservazione genuina dei suddetti dati. Infatti vi sono una serie di misure di sicurezza, previste dai Garanti europei, ritenute idonee a garantire l'autenticità dei dati. Rientrano tra queste misure: l'individuazione dei virus e l'attività di *screening* per il riconoscimento degli *spam*[166]. In caso di mancato espletamento dei controlli appena citati, all'*Internet Service Provider* si può addebitare una responsabilità civile con conseguente rischio sanzionatorio.

All'indomani del d.lgs. 132 del 2021, anche il Garante per la protezione dei dati personali ha espresso un parere negativo sull'accostamento delle due modifiche con specifico riferimento al principio di proporzionalità. Per il Garante, quindi, la procedura di acquisizione dei dati, così come modificata dalla riforma del 2021, esigerebbe una procedura di conservazione parimenti proporzionata. Nel suo Parere il Garante evidenzia come sia necessaria una variazione del termine di conservazione dei dati, con lo scopo di ricondurlo entro termini "maggiormente compatibili con il canone di proporzionalità"[167].

Dalle critiche fino ad ora sollevate si può affermare che la scelta migliore, ma al tempo stesso difficile e complessa, sia quella di stabilire una tempistica che bilanci da un lato le esigenze relative al diritto alla *privacy* e dall'altro le esigenze di natura investigativa, anche considerando le tempistiche attuali della giustizia italiana. Si potrebbe considerare valida l'ipotesi secondo la quale la scelta, ottimale, potrebbe essere quella di sottoporre tutti i dati conservati dagli *Internet Service Provider,* senza quindi distinzione tra dati di traffico telefonico e telematico, ad una scadenza

[166] Come stabilito dal Garante per la *Privacy* nel Parere 2/2006 sugli aspetti di tutela della vita privata inerenti ai servizi di screening dei messaggi di posta elettronica del 21 febbraio 2006.
[167] Critica mossa dal Garante delle *Privacy* nel Parere sullo schema di decreto-legge per la riforma della disciplina di acquisizione dei dati relativi al traffico telefonico e telematico a fini di indagine penale, 10 settembre 2021.

di trentasei mesi[168]. Quest'ultima andrebbe comunque coordinata con la disciplina europea del contrasto al terrorismo[169]. Ulteriormente sarebbe necessario inglobare questa riforma, che tanto si attende, in un pacchetto di aggiornamento dell'intera disciplina della "*data retention*" con conseguente possibilità di modificare in futuro le tempistiche, prevedendo una velocizzazione dei tempi in ambito processual-penalistico.

Quest'unico termine fissato a trentasei mesi riduce quindi la disparità di trattamento riguardante i dati del traffico telefonico e i dati del traffico telematico. Nonostante recentemente i progressi della tecnologia abbiano causato un mutamento del *"modus operandi*" dei criminali i quali ricorrono sempre più a modalità e strumenti evoluti, l'utilizzo dei dispositivi smartphone non solo come mezzo di comunicazione telefonica, ma anche come mezzo di comunicazione tramite applicazioni di messagistica telematica[170], resta un elemento centrale della criminalità. Per cui si è inclini ad appoggiare la tesi di quella scuola di pensiero che, successivamente all'entrata in vigore del d.lgs. 10 agosto 2018 n. 101, propendeva per ritenere illogico ed insensato sottoporre a due termini differenziati le due tipologie di dato. Eliminando con questa proposta lo scaglionamento introdotto nel 2018, si conservano i dati per una fascia temporale unitaria con meno spese anche per i fornitori del servizio.

Secondo l'impostazione dell'art. 132 codice *privacy*, il modello di conservazione impostato dall'Italia risponde ad una logica di "tipo automatico, generalizzato ed

---

[168] S. 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*., 11/2018, p.160.

[169] In una recente audizione davanti al Copasir, il 25 luglio 2017 (comitato parlamentare per la sicurezza della repubblica), il presidente del Garante per la protezione dei dati personali, Antonello Soro, all'indomani della approvazione della legge europea 20 novembre 2017, n. 167, ha spiegato come si auspichi un intervento del legislatore affinché possa ricondurre l'intera disciplina al criterio della proporzionalità.

[170] Come emerge dall'indagine "indice della criminalità" eseguita dal "*Sole e 24 Ore*" e riportata da F. BANFI*, Quali sono i reati informatici più diffusi? I reati informatici più diffusi: alcune statistiche*, in *Diritto Consenso*, aprile 2023. In questo articolo l'autore evidenza alcuni dati statistici importanti: i reati informatici sono cresciuti, nell'ultimo decennio, del 10,1%. Nel 2021 si registra una media di 800 reati informatici al giorno in tutta Italia, con picchi nelle città del nord.

indifferenziato[171]", in contrasto con la recente giurisprudenza della Corte di Giustizia[172], la quale ha statuito in merito alla contrarietà del modello di conservazione a natura indifferenziata e ha invitato gli Stati Membri ad adottare modelli di conservazione che mirino a criteri più specifici[173].

Le argomentazioni appena illustrate valgono a riprova dal fatto che il termine di settantadue mesi, corrispondente a sei anni, raffigura una scadenza molto dilatata nel tempo, contrastante sia con le scelte interne del Governo sia con le scelte di altri paesi europei. Gli esperti discutono da tempo su un eventuale cambiamento della disciplina, con correzione delle problematiche qui illustrate.

In conclusione, si attende un cambiamento riformistico in questo senso.

3. 2 Il rapporto con il principio di ragionevole durata del processo

Questa disciplina e le sue tempistiche dilatate nel tempo, derivanti dalle modifiche apportate dal d. lgs. 10 agosto 2018 n. 101, contrastano anche con il principio della ragionevole durata del processo sancito sia a livello internazionale, all'art. 6 della Convenzione Europea dei Diritti dell'Uomo, sia a livello nazionale, all'art. 111 della Carta Costituzionale. Secondo queste previsioni, un soggetto ha diritto "ad un'equa e pubblica udienza entro un termine ragionevole, davanti ad un tribunale

[171] Cit. R. FLOR-S. MARCOLINI, *Dalla* data retention *alle indagini ad alto contenuto tecnologico: la tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato,* Giappichelli, 2022, p. 47.
[172] Corte giust. UE, Grande Sezione, 5 aprile 2022, "*Commissioner*", C-140/20.
[173] Come ad esempio criteri basati sul dato geografico o su dati personali.

indipendente e imparziale costituito per legge"[174] e "la legge ne assicura la ragionevole durata"[175].

La norma costituzionale vincola il legislatore, il quale ha previsto delle norme a tutela dell'individuo che, coinvolto in un giudizio civile, penale o amministrativo, subisca dei danni patrimoniali o non patrimoniali a causa dell'irragionevole periodo di tempo trascorso in attesa del giudicato[176]. La ragionevole durata del processo viene vista, dalla maggior parte della dottrina, come una garanzia non soltanto in riferimento al soggetto coinvolto e al suo diritto di difesa, ma anche in relazione al buon andamento di tutta l'organizzazione della giustizia italiana[177]. Visto che "l'Italia è al primo posto, nel Consiglio d'Europa, per numero di condanne della Corte Europea dei Diritti dell'Uomo per irragionevole durata dei processi[178]" ed è stata più volte oggetto di procedure di infrazione da parte della Commissione Europea con conseguenti sanzioni, è ad oggi comprensibile la maturazione della volontà di ridurre drasticamente le tempistiche non solo del processo penale in senso stretto, ma anche di tutte le fasi delle indagini preliminari e del procedimento.

È opportuno esaminare anche un'ulteriore modifica[179] che è stata recentemente apportata alla disciplina della "*data retention*", la quale non è esente da critiche anche con riferimento al principio di ragionevole durata del processo e che ha appesantito la procedura di acquisizione dei dati esterni alle comunicazioni,

---

[174] In questi termini, si veda l'art. 6 della Convezione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali, firmata a Roma, 4 novembre 1950 e ratificata con l. 4 agosto 1955, n. 848.

[175] Così l'art. 111 della Costituzione della Repubblica Italiana, promulgata il 27 dicembre 1947 ed entrata in vigore il 1°gennaio 1948.

[176] L. 24 marzo 2001, n. 89. Entrata in vigore il 18 aprile 2001 e denominata "Previsione di equa riparazione in caso di violazione del termine ragionevole del processo e modifica dell'articolo 375 del codice di procedura civile". La cosiddetta "Legge Pinto" ha subito numerose modifiche sia nel 2012 che nel 2016 al fine di razionalizzare i costi conseguenti alla violazione del termine di ragionevole durata dei processi.

[177] Per approfondimenti, P. FERRUA, *La ragionevole durata del processo tra Costituzione e Convenzione europea*, in *Quest. giust.*, 1/2017.

[178] G.L. GATTA, *Lentezza dei processi e giustizia penale come tela di Penelope*, in "*Sole 24 Ore*", 2023.

[179] D. lgs 30 settembre 2021, n.132 recante "Misure urgenti in materia di giustizia e difesa, nonché proroghe in tema di referendum, assegno temporaneo e IRAP".

ampliando notevolmente le tempistiche investigative coinvolgendo il controllo giurisdizionale. Si è inclini a reputare la modifica in controtendenza rispetto all'idea di economia processuale.

Questa modifica, pertanto, non sembra rispettare il principio della ragionevole durata del processo anche per ragioni di organizzazione degli stessi uffici dei Tribunali e delle Corti d'Appello. Il giudice che si occupa dell'autorizzazione della richiesta del Pubblico ministero per l'acquisizione dei dati è il Giudice per le Indagini Preliminari, il quale è chiamato a decidere sulle richieste effettuate dal Pubblico Ministero, dalle parti private e dalla persona offesa durante la fase delle indagini preliminari e vigila anche sulla legalità degli atti delle stesse. Rispetto quindi alla procedura di acquisizione dei dati anteriore a questa disciplina riformistica, il procedimento è stato, secondo una parte della dottrina, appesantito con l'aggiunta di un passaggio ulteriore. Infatti, precedentemente la riforma del 2021, il Pubblico Ministero procedeva autonomamente disponendo l'acquisizione dei dati esterni alle comunicazioni, anche considerando la stessa figura del Pubblico Ministero in quanto titolare delle indagini e obbligato ad esercitare l'azione penale. Si può notare come la procedura risultasse, sicuramente, più veloce rispetto a quella odierna.

Il problema di fondo ha natura prettamente organica: i Tribunali dispongono di organico ridotto e di pochi G.i.p[180]. Dal canto suo il Ministero della Giustizia ha predisposto una serie di misure per aumentare l'organico dei Tribunali con lo scopo di ridurre notevolmente i tempi della giustizia e rispettare così l'impegno assunto anche a livello europeo con la firma del "Piano Nazionale di Ripresa e Resilienza". A fronte di un simile scenario, risulta antinomico, prettamente dal punto di vista di

[180] Questi i dati diffusi dal C.s.m. in data 28 luglio 2023 e riportati dal "*Sole 24 Ore*" il 5 agosto 2023 in merito: "In tutta Italia mancano 1652 magistrati. Rispetto ai 10633 posti previsti nell'organico, la scopertura nazionale è pari al 15,54%. A soffrire di più sono le Procure, con il 16% dei posti vacanti: su 2649 PM previsti sulla carta, ne mancano 426. Ma anche i Tribunali e le Corti d'Appello non se la passano bene: mancano 1226 giudici dei 7984 fissati nell'organico, con una scopertura pari allo 15,36%".

economia processuale, il motivo che ha spinto il legislatore ad introdurre una modifica che aggiunga un ulteriore passaggio nella procedura. Sicuramente, la scelta è dettata da intenzioni di giurisdizionalizzazione della procedura di acquisizione, ravvisando così una "svolta garantista"[181] operata dal legislatore stesso. In particolare, taluni autori ritengono che suddetta procedura, così rielaborata, possa facilitare l'utilizzo di questa importante fonte investigativa, ritenendo comunque possibile un rallentamento dell'ordinaria organizzazione degli uffici di Tribunali e Procure. Di conseguenza, ritengono che un "irrigidimento, pur ragionevole e proporzionato", determini "una maggiore salvaguardia dei diritti fondamentali"[182].

Le eventuali correzioni che si possono apportare alla disciplina sono già, da molto tempo, argomento di grande interesse per gli esperti in materia.

Ad oggi, a parere di chi scrive, appare condivisibile la tesi di parte della dottrina che ritiene la necessità dell'autorizzazione da parte del G.i.p. in contrasto con la volontà di riportare la giustizia all'interno di tempistiche ragionevoli e un inutile ed eccessivo irrigidimento della procedura stessa. Sarebbe stato opportuno attendere *in primis* le modifiche indirizzate alla velocizzazione dei tempi della giustizia e all'aumento dell'organico negli uffici, e *in secundis* apportare un significativo cambiamento alla disciplina di acquisizione dei tabulati, ricorrendo solo in quella circostanza ad un eventuale inasprimento della procedura. Inasprimento che probabilmente non sarebbe stato percepito come tale, se gli impegni presi dallo Stato in un'ottica di ragionevole durata del processo fossero stati mantenuti. Di

---

[181] G. FORMICI, "The three Ghosts of data retention*": passato, presente e futuro della disciplina italiana in materia di conservazione e acquisizione dei metadati per scopi investigativi. Commento a margine del d.l. 30 settembre 2021, n. 132 e relativa legge di conversione*, in *Osservatorio Costituzionale,* 1/2022, p. 153.

[182] Così G. FORMICI, "The three Ghosts of data retention*": passato, presente e futuro della disciplina italiana in materia di conservazione e acquisizione dei metadati per scopi investigativi. Commento a margine del d. lgs. 30 settembre 2021, n. 132 e relativa legge di conversione*, in *Osservatorio Costituzionale*, 1/2022, p. 153. Per approfondimenti, G. BATTARINO*, Acquisizione di dati di traffico telefonico e telematico per fini di indagine penale: il decreto-legge 30 settembre 2021, n. 132*, in *Quest. giust.*, 2021.

conseguenza si potrà giustificare una procedura che non risulterà appesantita, ma che sarà coerente con la salvaguardia di diritti fondamentali e con la ragionevole durata dei tempi processuali.

Con riferimento ad entrambe le problematiche, la disciplina necessita di correzioni. Si ritiene che il profilo delle tempistiche sia di notevole importanza visto come si intreccia anche con principi previsti sia dalla nostra Costituzione sia dalle Carte internazionali. È necessaria quindi un'armonizzazione delle esigenze di questa procedura con gli altri diritti che vengono in rilievo[183]. È comunque pacifica l'estrema difficoltà di apportare correzioni alla disciplina in materia di "*data retention*", visto anche il necessario coordinamento con normative di matrice europea. Si auspica, quindi, un intervento unitario che risolva tutte queste criticità.

3. 3 Il controllo del giudice: profili di incompatibilità della figura dei G.i.p. a seguito del d. lgs. 30 settembre 2021, n. 132

La nuova procedura di acquisizione dei metadati richiede un decreto motivato del G.i.p a seguito di richiesta da parte del Pubblico Ministero o su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private. Come già accennato, il G.i.p. svolge un'attività di garanzia durante tutto il periodo delle indagini, senza autonomi poteri istruttori e i suoi atti sono previsti dalla legge. Al termine delle indagini, si apre difronte al Pubblico Ministero una scelta: qualora non vi sia la possibilità di condanna del soggetto all'esito del processo avanzerà richiesta di archiviazione, la quale necessita di accoglimento del giudice, non potendo il Pubblico Ministero esercitarla

[183] Si fa riferimento al diritto di difesa, visto che dai tabulati si possono ricavare dati che potrebbero assumere valore di prova sia a carico che a discarico.

d'ufficio[184]; se invece, gli elementi acquisiti nel corso delle indagini consentono di formulare una ragionevole previsione di condanna, avremmo la predisposizione, da parte del G.i.p., del decreto di rinvio a giudizio[185].

Posteriormente all'entrata in vigore del d. lgs 30 settembre 2021 n. 132, con riferimento al procedimento di archiviazione, è sorta un'ipotesi di possibile incompatibilità della figura del G.i.p. Nello specifico, l'art 409 c.p.p. prevede due procedimenti distinti di archiviazione: l'archiviazione c.d. "*de plano*" ovvero l'immediato accoglimento da parte del G.i.p dell'istanza presentata dal Pubblico Ministero; ed un ulteriore procedimento di archiviazione che si verifica quando il G.i.p non accoglie subito la richiesta del Pubblico Ministero, perché intende svolgere altre indagini o perché ritiene che certi aspetti non siano stati adeguatamente approfonditi da parte del Pubblico Ministero. È necessario tenere in considerazione che, al termine di queste indagini aggiuntive, il Pubblico Ministero può ritenere consolidata la ragionevole previsione di condanna e richiedere così al G.i.p l'emanazione del decreto di rinvio a giudizio.

È necessario, prima di proseguire, chiarire che cosa s'intende per incompatibilità della figura del giudice. Il giudice, nell'esercizio delle sue funzioni, deve essere terzo ed imparziale[186]. Queste due qualità non devono intendersi come un'endiadi, in quanto con l'espressione "terzo" ci si riferisce all'autonomia del giudice all'intero di tutta l'organizzazione dell'ordinamento giudiziario, mentre il termine "imparziale" attiene all'estraneità dello stesso rispetto agli interessi in gioco in un dato procedimento. La legge ha introdotto una serie di meccanismi[187] a tutela

[184] Poiché verrebbe meno al suo dovere di esercitare l'azione penale in quanto titolare della pretesa punitiva dello stato, come previsto dall'art 112 Cost.
[185] D. lgs 150/2022, *Riforma Cartabia*, entrata in vigore il 30 dicembre 2022. Secondo parte della dottrina, la richiesta di archiviazione formulata dal Pubblico Ministero deve tenere conto della ragionevole previsione di condanna grazie agli elementi acquisiti nel corso delle indagini, anticipando così il superamento della presunzione di non colpevolezza. Precedentemente, invece, il potere di compiere le valutazioni in merito alla qualità degli elementi di prova forniti era devoluto ai G.i.p.
[186] Come stabilito dall'art. 111 Cost.
[187] Per l'imparzialità del giudice inteso come collegio giudicante, si vedano le norme relative alla remissione del processo, art. 45 c.p.p. I meccanismi, invece, a tutela dell'imparzialità del giudice

dell'imparzialità del giudice. Il meccanismo dell'incompatibilità, previsto all'art. 34 c.p.p., scatta in automatico quando il giudice svolge funzioni stabilite dallo stesso articolo che in qualche modo inficerebbero la sua imparzialità[188]. Si tratta di casi in cui il giudice potrebbe risultare condizionato da una sua scelta precedentemente adottata. Come si evince dalla lettura della norma, non vi è espresso riferimento al decreto motivato del G.i.p che autorizza l'acquisizione dei dati esterni alle comunicazioni, nonostante si possa individuare una forma di incompatibilità anche con riferimento a questo atto giudiziario.

Se questa forma di incompatibilità, illustrata in seguito, dovesse ritenersi valida, allora sarà opportuno apportare una modifica all'impostazione della norma.

L'eventuale problema di incompatibilità sorge proprio in questa evenienza: un G.i.p chiamato a rilasciare un decreto autorizzativo all'acquisizione dei metadati, ritenuti anche da lui stesso importanti per la prosecuzione delle indagini, in presenza di richiesta di archiviazione del Pubblico Ministero potrebbe non risultare d'accordo con la valutazione eseguita dal Pubblico Ministero stesso e, di conseguenza, fissare un ulteriore udienza come previsto dall'art. 409 c.p.p. Il dubbio di cui si discute e che sorgerebbe spontaneo è il seguente: il G.i.p. potrebbe essere condizionato dalla sua precedente scelta di autorizzare con decreto motivato l'acquisizione di dati ritenuti dallo stesso importanti ai fini delle indagini, tanto da non accogliere un eventuale richiesta di archiviazione presentata dal Pubblico Ministero?

Questa forma di incompatibilità risulterebbe adattabile anche ad altre procedure che prevedono un decreto motivato autorizzativo di una richiesta presentata dal Pubblico Ministero. In particolare, ci si riferisce al procedimento di acquisizione delle intercettazioni[189], il quale prevede lo stesso schema dell'art. 132 codice

---

inteso come persona fisica sono l'incompatibilità (art. 34 c.p.p. e ss.), l'astensione (art. 36 c.p.p.) e la ricusazione (art. 38 c.p.p.)

[188] La norma comprende l'emanazione della sentenza, l'emissione del provvedimento conclusivo dell'udienza preliminare o del decreto penale di condanna, la disposizione del giudizio immediato o la decisione in merito all'impugnazione avverso la sentenza di non luogo a procedere.

[189] Art. 267 c.p.p.

privacy: alla richiesta del Pubblico Ministero ne consegue la necessaria autorizzazione da parte del G.i.p. con decreto motivato. Un'altra procedura accostabile è quella prevista in ambito di sequestro, in cui è previsto che "l'autorità giudiziaria disponga il sequestro del corpo del reato e delle cose pertinenti al reato con decreto motivato[190]". Di conseguenza, questa forma di incompatibilità del G.i.p, qui trattata, si potrebbe individuare anche in queste procedure in quanto caratterizzate da un possibile condizionamento del giudice in sede di decisione circa l'acquisizione delle intercettazioni e la predisposizione di un sequestro.

L'incompatibilità derivante da atti compiuti nello stesso procedimento, che è la forma di incompatibilità di questa possibile situazione, non è solo quella prevista dall'art. 34, ma è anche quella derivante da numerose pronunce[191] delle Corte Costituzionale che hanno ampliato il raggio d'azione dello stesso meccanismo. La *ratio* sottostante a queste pronunce è la seguente: se un giudice, in una data fase del procedimento, è stato investito della questione relativa all'alternativa tra colpevolezza ed innocenza, responsabilità o non responsabilità, allora non potrà partecipare alle fasi successive. La Corte ritiene così che il giudice sia psicologicamente condizionato dalle sue stesse scelte.

Ritornando all'art. 409 c.p.p., al termine di questa udienza vi sono differenti esiti: o il giudice si convince della qualità delle indagini e dispone con ordinanza l'archiviazione; oppure ravvisa l'incompletezza degli elementi di prova e ordina lo svolgimento di ulteriori indagini con un termine; infine, ed è l'ipotesi più discussa, il giudice può ritenere che vi siano gli elementi per l'esercizio dell'azione penale arrivando ad ordinare la formulazione dell'imputazione, la c.d. imputazione coatta.

Ecco quindi la domanda: si può parlare di incompatibilità di un G.i.p, che precedentemente autorizza l'acquisizione dei tabulati, e successivamente alla richiesta di archiviazione del Pubblico Ministero non la accoglie perché

[190] Art. 253 c.p.p.
[191] Tra esse, Corte cost. 6 luglio 2001, n. 224 e Corte cost. 9 luglio 2013, n. 183

condizionato dalla sua precedente decisione? Come potrà mai essere solida un'azione penale derivante da un'imputazione coatta? È una completa ingerenza del giudice nell'attività di indagine del Pubblico Ministero, il quale dovrà ottemperare all'ordine impartitogli dal giudice per non incorrere in provvedimenti disciplinari o, ancor più grave, nel reato di abuso d'ufficio.

Il rischio che potrebbe verificarsi quindi è che, da un lato, l'azione penale risulti debole, e dall'altro, l'accusa possa apparire professionalmente poco convinta. Ad esempio nei casi in cui il processo prevede l'udienza preliminare, inevitabilmente si concluderà con una sentenza di non luogo a procedere, rivelandosi un'udienza inutile con deleterie perdite di tempo per tutto il sistema giudiziario.

In tutti in casi in cui ricorre un'ipotesi di incompatibilità prevista dall'art. 34 c.p.p, il giudice ha l'obbligo di astenersi con relativa dichiarazione presentata al presidente della Corte o del Tribunale. Se questo non avviene, e il giudice manifesti indebitamente il proprio convincimento sulle questioni del procedimento, allora interviene l'istituto della ricusazione[192]. Le parti presentano una dichiarazione scritta indicando i motivi e le prove che sostengono l'istanza di ricusazione.

Con riferimento a quanto detto sopra, si ritiene che questa eventuale incompatibilità ravvisata in sede di udienza a seguito di richiesta di archiviazione corrisponda ad una manifestazione, da parte del giudice, del proprio convincimento per cui è possibile che si concretizzi in una richiesta di ricusazione.

Come ulteriore soluzione al problema, si potrebbe proporre una leggera modifica alla procedura di archiviazione. Per cui, nel caso in cui il Pubblico Ministero presenti istanza di archiviazione al giudice che precedentemente aveva autorizzato l'acquisizione dei metadati, per evitare questa forma di incompatibilità sarebbe opportuno che la richiesta di archiviazione fosse presentata dinnanzi ad un diverso G.i.p.

[192] Art. 37 c.p.p.

Questo espediente però presenta dei profili problematici. Come esaminato nel paragrafo precedente, il problema della carenza di organico rileva sotto molteplici aspetti, per cui può accadere che non ci siano sufficienti giudici per supportare questa modifica. Inoltre un'ulteriore criticità presenta caratteri più pragmatici: vi è l'assoluta certezza che un secondo giudice non sia comunque influenzato dalla decisione riguardante l'autorizzazione all'acquisizione dei metadati e non si spinga anche lui a dilatare i tempi dell'archiviazione, con il rischio di giungere ad una imputazione coatta?

Ad oggi, gli esperti non si sono ancora pronunciati sulla esistenza o meno di un'aggiuntiva forma di incompatibilità derivante dall'introduzione della procedura di acquisizione dei metadati ex d.lgs. 30 settembre 2021 n. 132. Molto probabilmente perché i profili problematici della riforma stanno emergendo solo recentemente. Il dibattito che potrebbe derivare sarà sicuramente interessante e porterà i giuristi ad interrogarsi facilmente su questa eventualità cercando successivamente un modo per risolverla.

3. 4 Potere discrezionale del giudice in relazione al criterio della gravità dei reati previsto dal d. lgs. 30 settembre 2021, n. 132. Uno sguardo al commento dell'Avvocato Generale Collins

La riforma apportata dal d.lgs. 30 settembre 2021 n. 132 ha inserito come presupposto per l'acquisizione dei metadati, la gravità del reato per cui si procede[193]. Questa scelta legislativa ha suscitato numerose critiche. Ed è proprio con riferimento ad essa che l'Avvocato Generale della Corte di Giustizia dell'Unione Europea Anthony Michael Collins, ha espresso delle riflessioni. Queste

[193] Art. 1 d.lgs 30 settembre 2021, n. 132: "… se sussistono 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 minaccia e disturbo alle persone col mezzo del telefono, quando la minaccia, la minaccia e il disturbo sono gravi…".

riflessioni muovono da principi e requisiti di proporzionalità e necessità indicati dalla stessa Corte in due celebri sentenze[194]: per sorreggere il rilascio dell'autorizzazione da parte del giudice per l'acquisizione dei dati, deve sussistere necessariamente un reato grave, in modo tale da legittimare l'ingerenza, a sua volta rilevante, nel diritto alla *privacy* dell'utente.

L'intervento dell'Avvocato Generale è stato chiesto a titolo esplicativo a seguito di un rinvio pregiudiziale alla Corte di Giustizia da parte del Tribunale di Bolzano, proprio sul requisito della gravità e sul tipo di controllo che eventualmente, *ex ante,* il giudice può svolgere.

Innanzitutto è necessario ricordare come nessuna fonte sembri prevedere una definizione di gravità del reato in rapporto alla disciplina della "*data retention*". Ciò si può spiegare con il fatto che il diritto penale, e nello specifico i reati e le relative sanzioni, rispecchiano la tradizione sociale di una nazione, con la possibilità di variare nel corso del tempo contemporaneamente al cambiamento della società.

Sulla base dell'interpretazione restrittiva data dalla giurisprudenza europea con riferimento al principio di effettività e proporzionalità, ecco che "l'obiettivo della lotta contro la criminalità grave deve sempre essere conciliato con il godimento dei diritti fondamentali in tal modo pregiudicati"[195]. Secondo il commento dell'Avvocato Generale, la normativa in materia di "*data retention*" dovrebbe prevedere un controllo preventivo da parte dell'autorità giudiziaria con lo scopo di armonizzare gli opposti interessi in gioco: da un lato le esigenze investigative; mentre dall'altro la tutela del diritto alla riservatezza. Il controllo che il giudice dovrebbe fare, secondo Collins, coinciderebbe con la ricerca di uno stato di equilibrio tra la necessità di indagine e la protezione del diritto alla *privacy*.

[194] Corte giust. UE, 2 marzo 2021, C-746/18, *H.K v. Prokuratuur* e Corte giust. UE, 2 ottobre 2018, C-207/16*, Ministero Fiscal*

[195] Così come riportato da G. FORMICI, *La direzione indicata dalle Conclusioni dell'Avvocato Generale Collins nel caso C-178/22*, in *Media Laws*, 2022, p.173.

Equilibrio necessario dato dal fatto che il controllo sui dati personali potrebbe tramutarsi in una ingerenza negativa sulla sfera personale di un soggetto.

Con riferimento alla concreta applicabilità dell'art. 132 codice *privacy*, novellato dalla modifica del 2021, l'Avvocato Generale individua due possibili livelli di controllo *ex ante* che il giudice può essere chiamato a svolgere in relazione al presupposto della gravità: nel caso in cui si tratti di minaccia o disturbo per mezzo del telefono, è giusto interrogarsi su un eventuale valutazione individuale del giudice sulla proporzionalità dell'ingerenza rispetto alla forma e alla natura concreta della molestia, in un'ottica più generale di lotta alla criminalità; qualora ci si rifaccia al requisito tangibile della reclusione non inferiore ai tre anni, il giudice si dovrà contenere, nella sua valutazione, alla sola compatibilità concreta. Ma anche in quest'ultima alternativa, il giudice non può esimersi dal valutare la proporzionalità dell'accesso ai dati in relazione ad un dato reato. Ne consegue che, sempre in linea con quanto afferma l'Avvocato Generale Collins, anche nel caso in cui sia prevista una soglia di applicabilità sancita sulla base di un requisito di gravità previsto espressamente dalla legge, è opportuno ipotizzare l'esistenza di un dovere in capo al giudice di effettuare una considerazione sulla proporzionalità dell'interferenza pubblica sui dati privati.

In conclusione, Collins finisce per affermare l'esistenza di un potere discrezionale in capo al giudice, con la conseguenza, non poco rilevante, che, da un lato l'acquisizione dei dati possa essere negata anche se la fattispecie è qualificabile come un reato che superi la soglia di gravità prevista dalla normativa, e dall'altro il giudice non sarà obbligato ad autorizzare all'ingerenza nemmeno nel caso in cui la soglia sia pacificamente superata a meno che non effettui un controllo sulla proporzionalità della stessa con esito positivo.

Questa discrezionalità consente al giudice di rivestire un ruolo importante, in quanto autorità di controllo, in modo tale da non ritenersi totalmente vincolato a

quanto espresso nella norma[196]. L'interpretazione sostenuta dall'Avvocato Generale quindi, attribuisce un significativo potere ai giudici nel controllo preventivo della proporzionalità dell'acquisizione dei metadati consentendoli di derogare alla scelta normativa adottata dal legislatore.

La questione centrale, dunque, è capire come poter modificare l'art. 132 codice *privacy* e, al tempo stesso, chiedersi se effettivamente è plausibile un controllo preventivo in capo al giudice, alla luce di queste considerazioni. Sicuramente, suscita alcune perplessità l'automatico consenso all'acquisizione dei dati al raggiungimento di una soglia di gravità che è stata oggetto di numerose critiche. Tuttavia, non si esclude che il presupposto della gravità del reato non sia una condizione necessaria per richiedere l'acquisizione dei dati, sebbene sia meglio definirla come "sufficiente", in quanto è preferibile accostarla al controllo del giudice.

Si può ravvisare, in questa impostazione, una visione garantista del diritto fondamentale alla riservatezza, esaminando così i fatti nella loro concretezza e stabilendo, caso per caso, se l'accesso a questi dati sia proporzionato al di là di quanto previsto dal legislatore. Inoltre il controllo *ex ante* risulterebbe a vantaggio e a giovamento anche contro i possibili abusi derivanti dall'utilizzo improprio del criterio della gravità.

In generale queste considerazioni espresse dall'Avvocato Generale Collins ci portano a concludere che il dibattito sulla "*data retention*" non sia ancora giunto al termine sia in Italia sia in Europa. Se questa forma di controllo preventivo del giudice venisse accolta anche da parte della giurisprudenza italiana e ottenesse l'appoggio ulteriore dei giuristi ed esperti del settore, è possibile che si arrivi ad una riscrittura dell'art. 132 codice *privacy*, così che si attribuisca valore alla

[196]"Ne emerge un rafforzamento del potere attribuito ai giudici, perché l'autorizzazione all'accesso resta comunque subordinata al controllo di proporzionalità svolto dai giudici stessi". G. FORMICI, *La direzione indicata dalle Conclusioni dell'Avvocato Generale Collins nel caso C-178/22*, in *Media Laws,* 2022, p.174-175.

discrezionalità del giudice, rispettando *in toto* i principi previsti dalla giurisprudenza della CGUE.

3. 5 Equilibrio necessario (ma possibile?) tra esigenze di sicurezza nazionale e diritto alla privacy

Uno stato di diritto deve garantire ai propri cittadini non solo la sussistenza di norme dedite alla repressione dei reati e della criminalità, ma anche di norme che tutelino i diritti fondamentali di ogni singolo individuo. La sicurezza viene intesa come un valore prioritario per la società, tale da incidere sulla comunità giuridica e sui bisogni di ognuno di noi. Può accadere, quindi, che per salvaguardare la sicurezza, in quanto ideale essenziale per la collettività, si causi la possibile compressione di alcuni diritti e libertà fondamentali.

In dottrina[197] è pacifica la riflessione secondo la quale la protezione dei dati personali sia l'elemento centrale del diritto alla vita privata, ma l'attenzione non può discostarsi dalle scelte normative intraprese dagli Stati. Quest'ultime, infatti, disciplinano finalità divergenti alla tutela del diritto in questione, nonostante sia stato da subito qualificato come fondamentale nell'ordinamento dell'Unione Europea[198].

Ad oggi, è lampante come il rapporto, in certi aspetti contrastante, tra sicurezza e garanzia dei diritti fondamentali sia da sempre oggetto di studi e dibattiti anche da

[197] F. ROSSI DAL POZZO, *La tutela dei dati personali nella giurisprudenza della Corte di Giustizia*, In *Eurojus*, 2018, p. 1 e ss.
[198] Sul tema sia autori italiani che europei. Tra questi, M. DE SALVIA, *Dati personali e sfera privata nella giurisprudenza della Corte europea dei diritti dell'uomo: ricostruzione sommaria delle linee-guida,* in M. FUMAGALLI MERAVIGLIA (a cura di)*, Diritto alla riservatezza e progresso tecnologico. Coesistenza pacifica o scontro di civiltà?*, Editoriale scientifica, 2015. Per la rappresentanza estera, C. MAGNUSSON SJOBERG, *Threats to personal data security: how does the EU protect its citizens?,* The European Union, Cheltenham, 2018 e M. P. GRANGER-K. IRION, *The right to the protection of personal data: the new posterchild of European Union citizenship*?, Civil Rights and EU Citizenship, Cheltenham, 2018.

parte del legislatore con lo scopo di creare una realtà processuale orientata verso una situazione di equilibrio. Con riferimento al processo penale, il diritto alla sicurezza è innegabilmente connesso all'attività di accertamento e repressione dei reati[199], tanto è vero che il nostro processo penale è concepito con finalità cognitive a tutela delle garanzie individuali, le quali infatti delimitano l'area di intervento del potere accusatorio pubblico.

Quando il diritto alla *privacy* di un individuo si riversa in un processo penale, assumendo una forza accusatoria importante, si può facilmente pensare che la sicurezza nazionale abbia prevaricato su questo determinato diritto fondamentale. Quindi con riferimento al diritto alla riservatezza[200], ecco che il rapporto con la sicurezza nazionale e l'interesse alla repressione dei reati, si presenta molto complesso.

Questa predisposizione antitetica tra sicurezza e diritti fondamentali dell'individuo, merita un chiarimento: come anzi detto, la sicurezza costituisce un valore importante perché su di essa si fonda la pacifica e civile convivenza dei cittadini; d'altra parte il diritto alla *privacy* è diventato la colonna portante delle società moderne e tecnologiche[201].

È importante interrogarsi sulla portata di questo conflitto poiché vi è il rischio che, se prevaricasse il diritto alla sicurezza sul diritto alla *privacy*, questo causerebbe la possibilità di ricorrere "ad un controllo di massa sull'intera collettività"[202] con il pericolo concreto di violare tutte quelle libertà fondamentali che, in quanto tali, si vorrebbero tutelare ad ogni costo. Il raggiungimento della situazione di equilibrio

---

[199] Anche se non sono espressamente previste all'interno della Costituzione, si possono rilevare leggendo sia l'art. 2 che l'art. 112 Cost.

[200] Art. 15 Cost. Art. 8 C.e.d.u. Art. 12 Dichiarazione Universale dei Diritti Umani.

[201] Ci si riferisce ai c.d. "nuovi diritti tecnologici" elaborati dalla Corte Costituzionale tedesca, ovvero il "diritto alla garanzia della segretezza e integrità dei sistemi informatici" e anche il "diritto all'autodeterminazione sull'uso dei dati personali".

[202] A. MALACARNE *Sicurezza e libertà: alla ricerca di un equilibrio impossibile?,* in A. MALACARNE-G. TESSITORE, *La ricostruzione della normativa in tema di* data retention *e l'ennesima scossa della Corte di giustizia: ancora inadeguata la disciplina interna?* in *A. pen.*, 2022, p.5.

risulta complesso anche a causa del continuo sviluppo tecnologico, che impedisce al legislatore di concentrarsi solo ed esclusivamente su un determinato panorama di strumentazione tecnologica probatoria. Di conseguenza, il legislatore interviene con una regolamentazione della suddetta strumentazione, la quale potrebbe risultare obsoleta, facendo a sua volta diventare la normativa appena attuata, ormai superata[203].

Chiaramente la *privacy* e la riservatezza, non devono essere intesi come diritti assoluti, bensì devono essere inseriti in un contesto complesso, caratterizzato da diritti anche contrapposti, che il legislatore cerca di bilanciare.

Nella c.d. direttiva *e-privacy*[204], il legislatore europeo oltre a prevedere il generale divieto alla memorizzazione e conservazione indeterminata dei metadati[205], individua anche un'eccezione[206], la quale consente agli stati di ricorrere a misure di limitazione del diritto alla riservatezza solo qualora questa restrizione risultasse proporzionata e finalizzata alla salvaguardia della sicurezza nazionale e alla repressione dei reati. Ecco quindi come le esigenze securitarie abbiano spinto il legislatore ad accostare alla regola generale un'eccezione, ammettendo quindi una costrizione del diritto alla *privacy*, controllata però dai principi di proporzionalità e necessità, rispettando così le linee guida della giurisprudenza europea.

In merito al concetto di sicurezza, la Corte di giustizia nella pronuncia *La Quadrature du Net*[207], ha fornito una distinzione tra i concetti di "sicurezza nazionale" e "sicurezza pubblica", tollerando solo nei riguardi della prima la

[203] Si fa riferimento qui ad "una sorta di "rincorsa disperata" del legislatore alla normativizzazione dell'ultima tecnica investigativa". A. MALACARNE*, Sicurezza e libertà: alla ricerca di un equilibrio impossibile?*, in A. MALACARNE-G. TESSITORE, *La ricostruzione della normativa in tema di* data retention *e l'ennesima scossa della Corte di giustizia: ancora inadeguata la disciplina interna?* in *A. pen.*, 2022, p. 7.
[204] Dir. 58/2002/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. Pubblicata in Gazzetta Ufficiale n. L 201 del 31 luglio 2002.
[205] Art. 5 Dir. 58/2002/CE.
[206] Art. 15 Dir. 58/2002/CE.
[207] Corte giust. UE, 6 ottobre 2020*, La Quadrature du Net* e altri, cause riunite C-511/18, C-512/18 e C-520/18.

conservazione dei dati per un dato periodo temporale. La sicurezza nazionale è concepita come "interesse primario di tutela delle funzioni essenziali dello Stato e degli interessi fondamentali della società"[208], ovvero tutte le "attività tali da destabilizzare gravemente le strutture costituzionali, politiche ed economiche o sociali di un paese"[209], con immediato richiamo agli attacchi terroristici. La sicurezza pubblica, invece, pensata come il pericolo generale delineato dal verificarsi di episodi di criminalità, non rappresenta una minaccia tangibile e fondata alla sicurezza dell'intera nazione tale da giustificare una normativa interna derogatoria alla regola generale dell'art. 5 della direttiva *e-privacy.* La riflessione della Corte in questo caso giustifica l'orientamento generatosi successivamente secondo il quale l'adozione di norme che interferiscono con la conservazione dei dati di traffico telefonico e telematico e che potenzialmente possano ledere il diritto alla *privacy*, sono sorrette dallo scopo primario di tutela della sicurezza nazionale e sono sottoposte alla condizione necessaria del controllo effettivo da parte di un organo terzo ed indipendente affinché accerti la presenza delle condizioni legittimanti la procedura[210].

L'impostazione data dalla Corte di giustizia non è stata seguita da una pronuncia[211] del *Conseil d'Etat* francese il quale, in un caso di censura della normativa interna dei tabulati telefonici, si è servito proprio dell'art. 15 della direttiva *e-privacy* per giustificare una memorizzazione totalitaria dei metadati sull'intero territorio nazionale, come risposta all'elevato e persistente rischio di attacco terroristico, visto che la Francia aveva già subìto numerosi attacchi di matrice terroristica tra il 2020 e il 2021. Numerose sono state le critiche. Il giudice amministrativo francese

---

[208] A. MALACARNE*, Sicurezza e libertà: alla ricerca di un equilibrio impossibile?*, in A. MALACARNE- G. TESSITORE, *La ricostruzione della normativa in tema di* data retention *e l'ennesima scossa della Corte di giustizia: ancora inadeguata la disciplina interna?* in *A. pen.*, 2022, p.32

[209] Corte giust. UE, 6 ottobre 2020*, La Quadrature du Net* e altri, cause riunite C-511/18, C-512/18 e C-520/18.

[210] R. FLOR-S. MARCOLINI, *Dalla* data retention *alle indagini ad alto contenuto tecnologico: la tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato,* Giappichelli, 2022, p. 6.

[211] Conseil d'Etat, 21 aprile 2021, *French Data Network et al*., n. 393099, n. 394922, n. 397844, n. 397581, n. 424717, n. 424718.

ha rovesciato il binomio regola-eccezione della direttiva *e-privacy*, consentendo alla sicurezza nazionale di prevaricare sul diritto alla riservatezza, senza contare che, quanto stabilito dalla Suprema corte amministrativa francese, si pone in netto contrasto con quanto affermato nella pronuncia *La Quadrature du Net*.

Un ulteriore critica viene sollevata dal giudice emerito della Corte di giustizia, Vilenas Vadapalas[212], il quale ha affermato che l'interpretazione abbracciata dal *Conseil d'Etat* francese sia dotata di scarsa capacità euristica[213] e di conseguenza non condivisibile, in quanto non riuscirebbe a contrastare in maniera evidente una reale minaccia alla sicurezza nazionale, visto che si basa solo sulla vaga paura di episodi violenti a matrice terroristica.

Il problema del bilanciamento tra il diritto alla sicurezza e le esigenze di sicurezza nazionale e i diritti fondamentali, in questo caso il diritto alla riservatezza, è stato trattato dalla Corte di giustizia con due sentenze. La sentenza *Digital Rights Ireland*[214] ha stabilito l'importanza del principio di proporzionalità con riferimento alla possibile ingerenza pubblica sui dati personali di un soggetto, al fine della repressione dei reati, chiarendo come non si possa ricorrere ad una conservazione "generalizzata e indifferenziata"[215] dei dati. L'altra pronuncia a cui si fa riferimento è la sentenza *Tele 2* e *Watson*[216], la quale afferma che la disciplina derogatoria prevista all'art. 15 della direttiva *e-privacy* deve essere intesa in senso restrittivo. Alla Corte sono stati sottoposti due quesiti: *in primis* un chiarimento sulla portata dell'eccezione per capire come gli Stati potessero intervenire sulla conservazione dei dati; *in secundis* si chiedeva se questa disciplina si potesse applicare in

[212] V. VADAPALAS, *Legal opinion*, 24 febbraio 2022, n. 10.
[213] A. MALACARNE*, Sicurezza e libertà: alla ricerca di un equilibrio impossibile?,* in A. MALACARNE-G. TESSITORE, *La ricostruzione della normativa in tema di* data retention *e l'ennesima scossa della Corte di giustizia: ancora inadeguata la disciplina interna?*, in *A. pen.*, 2022, p. 34.
[214] Corte giust. UE, 8 aprile 2014, *Digital Rights Ireland*, cause riunite C-293/12 e C-594/12.
[215] Cit. Corte giust. UE, 8 aprile 2014*, Digital Rights Ireland*, cause riunite C-293/12 e C-594/12.
[216] Corte giust. UE, 21 dicembre 2016, *Tele 2 e Watson*, cause riunite C-203/15 e C-698/15.

situazioni di pericolo alla sicurezza pubblica e di contrasto alla criminalità interna dello Stato.

Secondo la lettura restrittiva dell'eccezione data dalla Corte, gli Stati non possono intervenire con discipline che contrastino con la tutela della *privacy* per perseguire scopi diversi da quelli appositamente previsti dall'art.15 della direttiva *e-privacy*. Per cui un'ingerenza nella *privacy* di un individuo può essere giustificato solo con la lotta alla criminalità grave e con rilievo nazionale. In merito a questo punto, la Corte fornisce una sorta di *vademecum* ricordando così quali sono le condizioni che legittimano l'applicazione della deroga prevista all'art.15 della direttiva *e-privacy*: è necessario che la disciplina nazionale stabilisca, con regole accurate e rigorose, i requisiti delle misure di conservazione dei dati consentendo così agli utenti di proteggerli al meglio; in più, si specifica che la memorizzazione deve rispondere a criteri oggettivi di possibile minaccia alla sicurezza nazionale.

Con riferimento al secondo quesito, la Corte si rifà al carattere tassativo e restrittivo dell'art. 15 della direttiva *e-privacy* per cui nessun altro obiettivo, se non quelli previsti dalla stessa eccezione, sono idonei a sostenere un'ingerenza nella *privacy* degli utenti. Successivamente si richiama il principio di proporzionalità, quale criterio guida per l'accesso ai dati da parte delle autorità nazionali.

In conclusione, la Corte risolve la questione affermando che la protezione della *privacy* è, inequivocabilmente, superiore rispetto alle ragioni di sicurezza pubblica. I legislatori europei sono quindi obbligati a "prendere sul serio"[217] la tutela della *privacy*, dovendo sottoporre qualsiasi normativa che preveda una qualche interferenza nei confronti della riservatezza dei dati, alla rigidità dell'art. 15 della direttiva *e-privacy*.

[217] O. POLLICINO-M. BASSINI, *La Corte di giustizia e una trama ormai nota: la sentenza* Tele2 Sverige *sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, in *Dir. pen. cont.*, 2016, p. 10.

La giurisprudenza delle Corti internazionali converge verso una conclusione: in caso di assenza di una legge che stabilisca i casi e i modi per poter restringere il diritto alla riservatezza, nessuna attività investigativa di tipo intrusivo del diritto alla *privacy* sarà possibile; nel caso, invece, di realizzazione di un dettato normativo, sarà compito di questa determinare i limiti, i casi e le modalità di intrusione nella sfera della riservatezza, con chiarezza e nel rispetto del principio di proporzionalità[218].

I risultati fino ad ora analizzati vengono sostenuti anche dall'Avvocato Generale Campos Sanchez Bordona[219], il quale ricorda come gli strumenti a tutela della sicurezza devono rispettare tutte le garanzie previste da uno Stato di diritto. Si necessita di un ordinamento giuridico che difenda i diritti fondamentali e che, al tempo stesso, provveda anche alle esigenze della società.

Questo paragrafo si è aperto definendo il rapporto tra diritto alla sicurezza e diritto alla *privacy* come contrastante e ad oggi, si può pacificamente affermare che questi contrasti sussistono ancora e che la risoluzione del problema risulti tuttora lontana, anche a causa delle differenti oscillazioni di pensiero che caratterizzano questo contrasto.

A riguardo appare condivisibile l'impostazione[220] secondo la quale spetti alle Corti e ai legislatori dei singoli Stati individuare quella situazione di convivenza e di bilanciamento tra l'intervento dello Stato a difesa dei propri *cives* e i diritti fondamentali alla riservatezza e alla protezione dei dati personali sanciti a livello internazionale. Infatti, l'attenzione della Corte di Giustizia alla riservatezza e alla protezione dei dati personali e, più in generale, al diritto alla *privacy*, è la

[218] Questa tesi è sostenuta da R. FLOR-S. MARCOLINI, *Dalla* data retention *alle indagini ad alto contenuto tecnologico: la tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato,* Giappichelli, 2022, p. 68. E sempre da S. MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta,* in *Cass. pen.*, 2015, p. 787.
[219] Conclusioni alla causa *La Quadrature du Net.*
[220] Conclusioni dell'Avvocato Generale Saugmandsgaard Oe sul caso *Tele2*.

dimostrazione dell'intenzione di giungere all'auspicato bilanciamento tra interessi contrapposti, ovvero sicurezza nazionale e diritto alla *privacy*[221].

Si può concludere affermando come sia doveroso ricordare che, attualmente, sono sottoposti al vaglio della Corte di giustizia numerosi casi riguardanti le esigenze securitarie e la repressione dei reati in rapporto con la disciplina della "*data retention*", per cui tornerà a trattare l'argomento. La questione centrale su cui riflettere e a cui i legislatori devono prestare attenzione è: la Corte ribadirà nuovamente i principi e i concetti fino ad ora affermati, convincendosi della loro autenticità, o cambierà di nuovo la sua visione allontanando ancora di più la fine del lungo percorso inerente alla disciplina della "*data retention*"?

3.6 Il problema dell'inutilizzabilità dei dati di traffico telefonico e telematico e dell'inutilizzabilità della "prova incostituzionale" alla luce della recente giurisprudenza

Come già sollevato nei capitoli precedenti, la questione dell'inutilizzabilità degli elementi di prova, ovvero in questo caso dei dati di traffico telefonico e telematico acquisiti nel corso di un'indagine, riveste una importanza fondamentale nel procedimento penale.

È necessario esaminare più nello specifico la sanzione dell'inutilizzabilità. Prevista dalla disciplina nazionale all'art. 191 c.p.p., l'inutilizzabilità colpisce l'acquisizione degli elementi di prova avvenuta in violazione dei divieti stabiliti dalla legge, prevenendo il ricorso all'analogia[222]. Essa è inoltre rilevabile anche d'ufficio in ogni stato e grado del procedimento. Viene distinta dalla nullità[223], ma dal punto di vista

[221] R. FLOR-S. MARCOLINI, Data retention *e indagini ad alto contenuto tecnologico: la tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato*, Giappichelli, 2022, p. 123.
[222] G. ILLUMINATI-L. GIULIANI, *Commentario breve al codice di procedura penale, Libro Terzo, Titolo I,* Cedam, 2020, p. 758 e ss.
[223] Prevista agli artt. 179 c.p.p. e ss.

sistematico, viene qualificata da alcuni[224] come "vizio dell'atto cui consegue una sanzione processuale[225]", mentre da altri[226] come puro vizio di validità della prova in quanto connesso al principio di legalità con conseguente esclusione del valore probatorio dell'elemento in discussione[227], assicurando così un processo penale svolto in modo equo e conforme alla legge.

L'impostazione dell'art. 191 c.p.p., così come delineata dal legislatore, non fornisce però un criterio legale di riconoscimento delle ipotesi di inutilizzabilità. Si ritiene che spetti alla giurisprudenza colmare questo vuoto in via interpretativa, procedendo ad una verifica caso per caso alla ricerca di una possibile violazione di un divieto probatorio[228].

In relazione alla tassatività delle ipotesi di inutilizzabilità, parte della dottrina[229] segue un'impostazione rigida, secondo la quale, come per la sanzione della nullità, anche l'inutilizzabilità debba essere sottoposta al vaglio del principio di tassatività con la conseguenza rilevante che tutte le violazioni non comprese espressamente nella sanzione in questione, non possano per analogia essere sanzionate. Altra parte della dottrina[230], invece, non sostiene l'esistenza del principio di tassatività in relazione al concetto di inutilizzabilità a causa della mancanza di un riferimento normativo espresso e preciso. Viene quindi esclusa l'applicazione analogica della tassatività a causa delle difficoltà incontrate dal legislatore nell'individuare

---

[224] E. OBERTO, *L'inutilizzabilità della prova nel processo penale*, in *Ius Itinere*, maggio 2019, p. 2. Anche D. SIRACUSANO-F. SIRACUSANO, *Le prove*, in G. DI CHIARA-V. PATANÈ-F. SIRACUSANO (a cura di)*, Diritto processuale penale,* Giuffrè, 2018, p. 275 e ss.

[225] Cit. E. OBERTO, *L'inutilizzabilità della prova nel processo penale*, in *Ius Itinere*, maggio 2019, p. 2.

[226] D. CHINNICI, *L'inutilizzabilità della prova, tra punti fermi e profili controversi*, in *Dir. pen. proc.*, luglio 2014, p. 890.

[227]G. ILLUMINATI-L. GIULIANI, *Commentario breve al codice di procedura penale*, Cedam, 2020, p. 753 e ss.

[228] È opinione prevalente che il solo dato testuale, letterario dell'art. 191 c.p.p. non sia risolutivo. F. M. GRIFANTINI, *Il segreto difensivo nel processo penale*, Giappichelli, 2001, p. 275 e ss.

[229] In particolare, N. GALANTINI, *L'inutilizzabilità della prova nel processo penale*, in *Pubblicazione del Dipartimento di Scienze Giuridiche dell'Università di Trento*, Cedam, 1992, p. 46.

[230] V. P. TONINI, *Il valore probatorio dei documenti contenenti dichiarazioni scritte*, in *Cass. pen.* 1990, p. 2217.

specificatamente i casi di inutilizzabilità in numero determinato. Nello specifico, quindi, questa parte della dottrina afferma che eventuali casi di inutilizzabilità debbano essere ricercati, non nelle norme, ma nei singoli procedimenti probatori, ovvero in relazione agli obiettivi che si vogliono raggiungere con l'acquisizione di quel specifico elemento di prova.

Anche la Corte Costituzionale[231], ha affermato come la sanzione dell'inutilizzabilità si applichi in relazione a divieti probatori che mirano alla tutela e alla protezione di beni giuridici rilevanti. La Corte ha, infatti, ribadito come nullità ed inutilizzabilità siano fenomeni autonomi e non sovrapponibili, escludendo così la possibilità di applicare alla disciplina dell'inutilizzabilità concetti specifici e tipici del regime delle nullità, come la tassatività e il regime delle nullità derivate[232].

Inoltre si evince, dall'interpretazione della Corte di Cassazione, come il concetto di inutilizzabilità, e le norme ad esso riferite, siano state concepite come ulteriore strumento di tutela per l'imputato, evitando di conseguenza che elementi di prova acquisiti in maniera non conforme al dettato normativo possano avere effetti negativi nella sfera personale dell'imputato stesso[233].

Recentemente la Corte di Cassazione[234], si è espressa in relazione all'inutilizzabilità dei dati telefonici contenuti nei tabulati. Il difensore dell'imputato ha presentato ricorso presso la Suprema Corte deducendo l'inutilizzabilità ex art. 191 c.p.p. dei tabulati telefonici acquisiti in violazione dei divieti stabiliti dalla legge. Sempre secondo l'impostazione difensiva, i tabulati sarebbero inutilizzabili a causa del contrasto dell'art. 132 codice *privacy* con l'art. 15 della Direttiva 2002/58/CE, letto alla luce degli artt. 7, 8, 11 e 52 della Carta dei Diritti Fondamentali e alla luce dell'interpretazione della Corte di Giustizia nella sentenza del 2 marzo 2021 su caso

[231] Corte cost. 3 ottobre 2019, n. 219.
[232] Si intende la propagazione del vizio in successive fasi del processo.
[233] G. FIORUCCI, *Disorientamenti applicativi in tema di inutilizzabilità e tutela sostanziale del contraddittorio*, in *A. pen.*, settembre-dicembre 2022, p. 2-3.
[234] Cass., Sez. III, 1° aprile 2022, n. 11993.

H.K., riferendosi dunque al requisito della gravità del reato. Il reato in questione, previsto all'art. 609-*octies* c.p. non è ritenuto reato grave, per cui l'acquisizione dei tabulati non sarebbe proporzionata.

La Corte ritiene infondato il presente motivo di ricorso affermando che l'onere della prova è a carico di chi invoca l'inutilizzabilità: "chi invoca l'applicazione dell'art. 191 c.p.p. deve, dunque, provare il fatto da cui deriverebbe l'inutilizzabilità"[235]. In questo caso, quindi, la difesa per sostenere la sanzione dell'inutilizzabilità avrebbe dovuto presentare il fatto processuale in grado di sorreggere e giustificare la richiesta di dichiarazione di inutilizzabilità dei tabulati telefonici. Nello specifico, il fatto processuale da provare non è la produzione ed acquisizione dei tabulati, bensì l'acquisizione dei suddetti con decreto del Pubblico Ministero e non con decreto del giudice, con conseguente, e minuziosa, indicazione nel ricorso del decreto del Pubblico Ministero che ha autorizzato l'acquisizione dei tabulati, inserendo anche delle coordinate che consentano ai giudici di rinvenire il decreto autorizzatorio in questione all'interno degli atti processuali[236]. Dalla motivazione della sentenza emerge come la Corte abbia, comunque, effettuato un controllo sugli atti processuali alla ricerca del decreto autorizzatorio del Pubblico Ministero, con esito negativo[237].

Inoltre, la Corte non solleva dubbi nemmeno in relazione alla proporzionalità e alla compatibilità della disciplina nazionale precedente alle modifiche introdotte con il d. lgs. 30 settembre 2021, n. 132, con quella europea a seguito della sentenza sul caso H.K. Il reato in questione e i suoi limiti edittali[238] rientrano tra quelli previsti dall'attuale disciplina, anche a seguito dell'introduzione della legge di conversione.

---

[235] Così, Cass., Sez. III, 1° aprile 2022, n. 11993.
[236] Questo onere di specificità del ricorso è consolidato anche in giurisprudenza. Solo per citarne alcune: Cass., Sez. Un., 23 aprile 2009, n. 23868, Cass., Sez. Un., 16 luglio 2009, n. 39061, Cass., Sez. VI, 1° ottobre 2020, n. 37074.
[237] Considerando 2.5 della sentenza Cass., Sez. III, 1° aprile 2022, n. 11993.
[238] Il delitto di violenza sessuale di gruppo ex art. 609-octies c.p. era punito, all'epoca del commesso reato, con la reclusione da 6 a 12 anni. La pena è stata elevata nel 2019, con la legge n. 69, e quindi attualmente è punito con la reclusione da 8 a 14 anni.

Infine la Corte stabilisce che i tabulati sono sempre utilizzabili, anche se acquisiti prima delle modifiche apportate in questi ultimi anni, quando e se sono a favore dell'imputato[239]. Non si configura quindi una violazione di norme sull'acquisizione dei suddetti elementi di prova tale da causarne l'inutilizzabilità, poiché l'unico limite per la loro acquisizione si riscontrerebbe qualora quest'ultimi non fossero a favore dell'imputato.

Il ragionamento seguito dalla Corte attiene alla compatibilità tra la prova da acquisire, ed a favore dell'imputato, e il diritto tutelato dalla forma di inutilizzabilità di cui si discute, configurando così un'ennesima visione garantista.

È interessante notare come i giudici di legittimità abbiamo richiamato, in più punti della loro motivazione, la sentenza della Corte di Giustizia sul caso H.K. In particolare, è stato evidenziato come la Corte di Giustizia non abbia dato per assoluta la sanzione dell'inutilizzabilità dei dati, lasciando in realtà ai singoli Stati Membri delle scelte: "stabilire una inutilizzabilità *tout court* dei dati acquisiti in violazione della Direttiva 2002/58/CE, prevedere dei limiti ulteriori in tema di valutazione della prova, oppure infine inserire una valutazione in punto di dosimetria della pena."[240]

L'intervento successivo interno è stato quello di prevedere una disciplina secondo la quale i dati acquisiti prima delle modifiche normative del 2021, possano essere utilizzati solo unitamente ad altri elementi di prova e per l'accertamento di quei reati ricompresi nel requisito della gravità[241]. Su questa impostazione la Suprema Corte si è espressa positivamente affermando che si rafforza l'imparzialità del giudice, in quando figura deputata al controllo preventivo alla produzione del

[239] La sentenza stabilisce inoltre che questa disciplina, prevista dal legislatore, è del tutto compatibile con la normativa europea e con l'interpretazione corrente della Corte di Giustizia, essendo questa una disciplina fortemente garantista.
[240] Ne parla anche M. BUFFA, "*Data retention" e diritto transitorio: un possibile punto fermo giurisprudenziale,* in *Quest. giust.*, 2022.
[241] Sul punto anche D. ALBANESE, *La Corte di cassazione sulla legittimità della disposizione transitoria relativa alla nuova disciplina in materia di* data retention, in *Sistema Penale*, aprile 2022, p. 4.

decreto autorizzativo, e si rispetta la garanzia del contraddittorio, in quanto la difesa può produrre prove contrarie.

Questa pronuncia, condivisa dalla maggioranza della dottrina[242], suscita interesse per *l'iter* motivazionale seguito dai giudici di legittimità, in quanto viene chiarito, a livello giurisprudenziale, il problema della utilizzabilità dei tabulati acquisiti in vigore della previgente disciplina. È stato eseguito un controllo specifico in relazione al rispetto, da parte del legislatore nazionale, dei principi previsti dalla recente interpretazione della Corte di Giustizia nella sentenza del 2 marzo 2021 sul caso H.K.

Una ulteriore problematica concernente la sanzione dell'inutilizzabilità riguarda la cosiddetta "prova incostituzionale". Questa tipologia di prova, sostenuta da una parte della dottrina[243], è stata affermata per la prima volta dalla Corte Costituzionale con la sentenza n. 34 del 1973, accertando l'esistenza di "divieti" probatori ricavati da norme costituzionali. Di conseguenza fu stabilito che "attività compiute in dispregio dei fondamentali diritti del cittadino non possono essere assunte di per sé a giustificazione ed a fondamento di atti processuali a carico di chi quelle attività costituzionalmente illegittime abbia subito"[244].

Le prove incostituzionali sono quelle prove considerate inutilizzabili nel processo in quanto ottenute con modalità e comportamenti contrastanti con i diritti fondamentali previsti e garantiti dalla Costituzione. A differenza del principio del contraddittorio e della sua esclusione probatoria esplicitamente previsti all'art. 111 Cost., comma 4, in relazione ai suddetti divieti probatori non è ricavabile una

[242] Tra tutti, Marcello Buffa, giudice del Tribunale di Varese, e Giuseppe Battarino, ex magistrato presso il Tribunale di Varese.
[243] In quanto una parte, ad oggi minoritaria della dottrina, sosteneva quell'orientamento secondo il quale la Costituzione non potesse mai essere fonte di valutazioni di inutilizzabilità, poiché esse competono solo alla legge processuale. In caso di eventuali contrasti, si riteneva che fosse compito del legislatore intervenire nella sede opportuna. Questo orientamento è stato appunto superato dalla successiva impostazione presentata dalla Corte Costituzionale nella sentenza 34/1973. G. ILLUMINATI-L. GIULIANI, *Commentario breve al codice di procedura penale*, *Terzo Libro, Titolo I*, Cedam, 2020, p. 753 e ss.
[244] Corte cost., 4 aprile 1973, n. 34.

singola ed espressa norma processuale in Costituzione. La dottrina prevalente[245] tende a differenziare due forme distinte di prova incostituzionale: da un lato, si parla di prova acquisita in violazione di regole che stabiliscano l'esclusione probatoria prevista da norme processuali in Costituzione; dall'altro, invece, ci si riferisce alle prove viziate all'origine a causa di una violazione di qualsiasi norma costituzionale e del diritto fondamentale da essa tutelato. La soluzione prevalente prevede che per il primo caso si possa ipotizzare una diretta applicazione della norma costituzionale, violata con l'acquisizione di quell'elemento di prova, mentre in relazione al secondo caso, è ritenuto opportuno che il giudice, se intende affermare l'inutilizzabilità, debba sollevare questione di legittimità costituzionale.

Poiché l'art. 191 c.p.p. non indicherebbe tutti i casi di inutilizzabilità e dovendo fare necessariamente riferimento ad ulteriori criteri per individuare tali ipotesi di inutilizzabilità, in dottrina, alcuni[246] riconoscono l'importanza dell'interesse giuridico protetto da una data norma prevedendo quindi un'ipotesi di inutilizzabilità nei casi di violazione di divieti posti a garanzia dei diritti fondamentali previsti dalla Costituzione.

In relazione al rapporto tra inutilizzabilità e violazione della *privacy*, è configurabile la presente sanzione nei casi di violazione della regola di acquisizione dei dati a fini probatori[247]. È invece ritenuta causa di inutilizzabilità, l'uso dei relativi dati acquisiti in ambiti esterni e diversi da un procedimento penale[248].

---

[245] P. FERRUA, *Ammissibilità della prova e divieti probatori*, in *Revista Brasileira de Direito Porcessual Penal,* 2021, p. 238. Anche F. CAPRIOLI, *Colloqui riservati e prova penale*, Giappichelli, Torino, 2000, p. 236 e ss. e N. GALANTINI, *L'inutilizzabilità della prova nel processo penale,* Cedam, Padova, 1992, p. 204 e ss.

[246] G. ILLUMINATI-L. GIULIANI, *Commentario breve al codice di procedura penale*, *Terzo Libro, Titolo I*, Cedam, 2020, p. 759.

[247] Ne parla anche C. CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, Cedam, 2007, p. 120 e ss.

[248] Come stabilito da Parere del Garante della *privacy* sull'accesso ai dati telefonici: garanzie per le chiamate in entrata, introdotto il 3 novembre 2005.

Recentemente[249], la Corte di Cassazione si è nuovamente espressa su un ricorso, il quale poneva all'attenzione dei giudici di legittimità la questione relativa all'utilizzazione probatoria dei tabulati telefonici comprovanti la localizzazione dell'utenza telefonica dell'imputato, per dimostrare che questi al momento dei fatti si trovava in altro luogo. Nello specifico l'imputato reputava inutilizzabili i tabulati[250] in quanto acquisiti direttamente dalla Polizia Giudiziaria senza il decreto autorizzativo del giudice.

La Suprema Corte, nella sua motivazione, si riferisce ai casi di possibile tensione tra i diritti spettanti alle persone e il potere investigativo ed intrusivo dello Stato e dell'Autorità Pubblica. È opinione consolidata quella secondo la quale l'evoluzione sociale causi una costante creazione di nuove modalità di relazione tra lo Stato e i suoi cittadini. In virtù di ciò, la Costituzione è dotata di uno strumento a protezione dei diritti, ovvero l'art. 2, il quale con la sua stesura aperta e onnicomprensiva consente di proteggere un numero sempre più ampio di diritti fondamentali. Le altre aree della Costituzione fondamentali, nei rapporti tra Stato e cittadino, sono rinvenuti dalla Corte negli artt. 13, 14 e 15 con le relative riserve di legge e di giurisdizione, le quali assumono particolare importanza in relazione alla nascita di nuove forme investigative molto persuasive e infiltranti i diritti fondamentali delle persone. La Corte conclude questo *excursus* affermando nuovamente il concetto di prova incostituzionale, sottolineando come "la prova lesiva di diritti fondamentali, anche se atipica, è vietata e, se acquisita, è inutilizzabile"[251].

La Corte quindi conclude affermando che la sentenza è viziata sotto il profilo della procedura di acquisizione dei dati in questione, in quanto il decreto autorizzativo[252] del giudice all'acquisizione dei dati non è rinvenibile all'interno degli atti

[249] Cass., Sez. VI, 14 aprile 2023, n. 15836.
[250] Tabulati principalmente grazie ai quali, fu perfezionata la condanna.
[251] Considerando 2.2 Cass., Sez. VI, 14 aprile 2023, n. 15836.
[252] Anche in sede di giudizio abbreviato.

processuali[253]. Anche alla luce dell'interpretazione della Corte Costituzionale[254], la quale ha chiarito come l'art. 15 della Costituzione impedisca qualsiasi divulgazione dei dati esteriori delle comunicazioni facendone quindi oggetto di uno specifico diritto costituzionale alla tutela della sfera privata e della segretezza delle comunicazioni, ne deriva l'inutilizzabilità di quei tabulati o di quei dati di traffico telefonico o telematico assunti in violazione delle norme processuali che ne disciplinano la loro acquisizione, essendo appunto configurabili effetti negativi anche per i diritti costituzionali ed essi connessi.

Oltre all'inutilizzabilità derivante dal mancato rispetto delle norme inerenti alla procedura di acquisizione, la Suprema Corte[255] ha elaborato anche un'altra forma di inutilizzabilità in relazione alla violazione dei termini di conservazione dei dati. Questa impostazione giurisprudenziale ha trovato espresso riferimento normativo nell'art. 132, comma 3, codice *privacy*, individuando così una forma di inutilizzabilità patologica[256].

In conclusione, al soggetto che sceglie il mezzo telefonico, in virtù dell'art. 15 della Costituzione, va riconosciuto il diritto di mantenere segreti sia i dati esterni alla conversazione, sia quelli relativi all'ubicazione e al tempo della comunicazione. Secondo questa impostazione, si assicura al soggetto titolare del dispositivo garanzie sia tecniche che giuridiche. La giurisprudenza sia italiana che europea continua a garantire che gli elementi di prova siano acquisiti nel rispetto dei diritti

[253] Essendo la sentenza pronunciata nell'aprile 2022, la disciplina transitoria era già in vigore in quanto introdotta con la lg. 178 del 2021. Ricadeva sulla Corte d'Appello l'onere di verificare l'esistenza delle condizioni necessarie per procedere all'acquisizione dei tabulati, ovvero l'emissione del decreto autorizzatorio da parte del giudice. Per un commento, P. E. DE SIMONE, *La rilevanza probatoria dei tabulati telefonici comprovanti la localizzazione di un'utenza telefonica (c.d. "pedinamento elettronico")*, in *Jus*, aprile 2023, p. 1. E anche A. SCARCELLA, *Geolocalizzazione: no all'utilizzabilità dei tabulati se manca l'autorizzazione*, in *Il Quotidiano Giuridico*, aprile 2023, p. 2 e ss.

[254] Corte cost. 11 marzo 1993, n. 81.

[255] Cass., Sez. VI, 4 maggio 2006, n. 33435.

[256] R. FLOR-S. MARCOLINI, *Dalla* data retention *alle indagini ad alto contenuto tecnologico: la tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato,* Giappichelli, 2022, p. 6.

fondamentali, senza irrigidire ulteriormente le attività di indagine e di repressione dei reati.

Inoltre, è interessante esaminare anche la disciplina dell'utilizzabilità dei dati acquisiti in violazione delle disposizioni del codice *privacy*. Esaminando la relazione del Garante della *privacy*, in riferimento all'anno 2021[257], sono 2 071 le violazioni di dati personali, sia nel settore pubblico[258] che privato[259], notificate all'Autorità. In seguito, l'attività di natura istruttoria eseguita dall'Autorità ha dimostrato una duplice natura: da un lato, ha inteso esaminare l'adeguatezza delle misure di sicurezza previste dal titolare del trattamento per prevenire suddette violazioni o per porre rimedio ai possibili effetti negativi derivanti dalla stessa; dall'altro, ha valutato la necessità di informare i soggetti coinvolti, fornendo tutte le indicazioni necessarie in relazione alle misure da adottare per proteggersi dalle conseguenze.

Nello specifico, in merito all'utilizzo di banche dati accessibili al pubblico, con lo scopo di inviare messaggi di tipo promozionale, sono pervenute una serie di segnalazioni al Garante, il quale ha avviato una procedura istruttoria. All'esito dell'istruttoria, i reclami avanzati sono stati confermati, in quanto una società aveva reperito i contatti personali di numerosi professionisti servendosi di un registro pubblico, senza quindi il consenso dei soggetti interessati. Il Garante, in relazione all'utilizzabilità di questi dati, ha dichiarato l'illegittimità del trattamento, ha vietato la continuazione dell'attività promozionale, ed infine ha intimato alla società di cancellare i dati già acquisiti in violazione delle norme contenute nel codice *privacy*, in quanto la "finalità pubblica del registro non può ricomprendere anche l'attività di contatto promozionale"[260], la quale è consentita solo con il consenso del

[257] Relazione annuale 2021 del Garante della *privacy*, presentata al Senato il 7 luglio 2022.
[258] Nel settore pubblico, le violazioni hanno riguardato comuni, istituti scolastici e strutture sanitarie.
[259] Nel settore privato, sono state coinvolte sia piccole che medie imprese, nonché liberi professionisti e grandi società del settore delle telecomunicazioni, del settore energetico e bancario.
[260] Relazione annuale 2021 del Garante della *privacy*, paragrafo 13.3, *Raccolta di dati* online, p. 138, presentata al Senato il 7 luglio 2022.

contraente[261]. Un altro episodio di violazione dei dati personali, trattato dal Garante nella sua relazione, concerne la violazione dei sistemi di sicurezza delle piattaforme di *social-network*[262]. Infatti, a causa di questa violazione, numeri telefonici e indirizzi *e-mail* di milioni di utenti italiani, erano disponibili online. L'Autorità, con apposito provvedimento, ha avvertito chiunque fosse entrato in possesso di dati personali appartenenti agli altri utenti derivanti da questa violazione, che suddetti dati sono frutto di un trattamento illecito e, di conseguenza, il loro eventuale utilizzo si sarebbe concretizzato in un contrasto con la normativa prevista dal codice *privacy*, con conseguente rischio sanzionatorio.

Per concludere, sono stati presentati diversi reclami riguardanti la legittimità dell'acquisizione e successiva utilizzazione di dati personali in sede giudiziaria. L'Autorità ha chiarito che spetta al giudice verificare la conformità, del trattamento e dell'acquisizione dei dati personali, alle modalità previste dalle disposizioni di legge263. Fornendo ulteriori chiarimenti in merito ad uno specifico reclamo264, il Garante ha affermato che la norma di riferimento in relazione all'utilizzazione dei dati personali in un giudizio penale è l'art. 160-bis del codice privacy, rinviando così alle disposizioni processuali pertinenti. Infine, in relazione all'utilizzazione e successiva valutazione dei dati personali, il Garante precisa che non è di sua competenza l'attività di controllo, di conformità a quanto previsto dalle norme in materia, dei trattamenti effettuati dalle autorità giudiziarie durante l'espletamento delle loro funzioni.

[261] È quanto previsto dall'art. 130 del codice *privacy* in base al quale "l'invio di comunicazioni con modalità automatizzate è consentito solo con il consenso del contraente o dell'utente potendosi ammettere una deroga unicamente nel caso in cui l'indirizzo *e-mail* sia stato rilasciato dall'interessato nel contesto di una vendita di beni o servizi analoghi".
[262] Il Garante si riferisce al grave caso di *data breach* subito da *Facebook* nell'aprile del 2021.

3.7 Natura giuridica e principi costituzionali in comune con la disciplina delle intercettazioni

A questo punto dell'elaborato, è opportuno soffermarsi anche sulla disciplina delle intercettazioni[263], in quanto mezzo di ricerca della prova dotato di caratteristiche affini alla disciplina della *"data retention*", ma che al tempo stesso presenta delle criticità[264]. In particolare, ci si soffermerà sui principi costituzionali e sovranazionali che accomunano le due discipline, operativamente distinte[265], ma con basi giuridiche molto simili.

Un elemento che accomuna le due discipline è rinvenibile nei principi costituzionali di riferimento. Così come per la *"data retention*", anche per le intercettazioni, all'esigenza processuale di completamento del quadro indiziario, si contrappongono: il diritto alla *privacy* e il diritto alla riservatezza delle comunicazioni[266]. Ma non solo. Ulteriori principi di riferimento sono ricavabili da fonti sovranazionali come il diritto al rispetto della vita privata e della vita familiare[267], la libertà di espressione e di informazione[268] e il diritto al rispetto della dignità dei soggetti coinvolti.

---

[263] L'ultima riforma che ha investito la disciplina delle intercettazioni è il d. lgs. 30 dicembre 2019, n. 161 denominato Modifiche urgenti alla disciplina delle intercettazioni di conversazioni o comunicazioni. Decreto convertito con la l. 28 febbraio 2020, n. 7.

[264] Per un approfondimento completo sulle criticità della disciplina delle intercettazioni, L. FILIPPI, *Intercettazioni, accesso ai dati personali e valori costituzionali*, Processi e Procedimenti, Pacini *Giuridica*, 2021. Anche D. CURTOTTI, *La giurisprudenza europea*, P. MAGGIO, *I presupposti applicativi,* M. L. DI BITONTO, *La captazione di flussi informatici*, E. PILLA, *Provvedimenti e motivazione,* A. NOCERA-P. DI GERONIMO, *Esigenze di riservatezza: conservazione, modalità di stesura delle ordinanze e acquisizione del captato oltre le indagini preliminari*, N. GALANTINI, *L'inutilizzabilità dei risultati*, P. FELICIONI, *Le fattispecie "atipiche" e l'impiego processuale*, in (a cura di) T. BENE, *L'intercettazione di comunicazione*, Giustizia penale della post-modernità, Cacucci Editore, 2018.

[265] Nello specifico l'intercettazione consiste nella captazione di una comunicazione nello stesso momento in cui questa avviene, mentre in relazione alla "*data retention*", quello che avviene è un'acquisizione di dati conservati da parte dei fornitori dei servizi di comunicazione.

[266] Previsti all'art. 15 della Costituzione.

[267] Art. 7 della Carta dei Diritti Fondamentali dell'Unione Europea.

[268] Art. 11 della Carta dei Diritti Fondamentali dell'Unione Europea.

In relazione al diritto alla riservatezza, la disciplina delle intercettazioni, precedente alla riforma del 2019, presentava delle lacune e nello specifico dimostrava una differente calibrazione da parte del legislatore in riferimento al diritto alla riservatezza. In merito, la Corte Europea dei Diritti dell'Uomo[269] aveva inizialmente indicato una serie di requisiti, da lei ritenuti essenziali, per raggiungere un livello di protezione adeguato. Tra questi è opportuno citare: la definizione delle categorie dei soggetti passivi all'intercettazione; la fissazione di un termine massimo per la durata delle intercettazioni; ed infine, la predisposizione di una disciplina apposita concernente le precauzioni da adottare affinché venga garantita la riservatezza dei soggetti interlocutori che vengano casualmente intercettati e che siano totalmente estranei all'oggetto delle indagini[270].

Di conseguenza, come è accaduto per la disciplina della "*data retention*", le interpretazioni delle Corti sovranazionali[271] spingevano per la realizzazione di una disciplina delle intercettazioni che mantenesse in equilibrio, da un lato, il diritto alla vita familiare ed alla *privacy*, e dall'altro, l'interesse generale dello Stato al perseguimento dei reati. Quindi, anche nell'ambito delle intercettazioni, la tutela della riservatezza e la protezione dei dati personali dei soggetti coinvolti vengono intesi come "beni inviolabili"[272], con l'obbligo di salvaguardarli[273].

Così come precisato da tempo dalla Corte Europea dei Diritti dell'Uomo[274], la quale è intervenuta più volte, lo strumento investigativo delle intercettazioni rientra nell'ambito di operatività dell'art. 8 CEDU, sotto il profilo del rispetto e della

[269] In una serie di pronunce, tra cui: Corte eur. 30 luglio 1998, *Venezuela Contreras c. Spagna* e Corte eur. 16 febbraio 2000, *Amann c. Svizzera*.
[270] Per l'elenco completo, L. FILIPPI, *Intercettazioni, accesso ai dati personali e valori costituzionali*, Processi e Procedimenti, Pacini Giuridica, 2021, p. 17.
[271] Corte eur. 30 aprile 2013, *Cariello e altri* c. *Italia*.
[272]Cit. L. FILIPPI, *Intercettazioni, accesso ai dati personali e valori costituzionali*, Processi e Procedimenti, Pacini Giuridica, 2021, p. 18.
[273] Infatti, è rinvenibile nella riforma in materia di intercettazioni un rafforzamento del segreto a tutela della riservatezza. Per un approfondimento, L. FILIPPI, *Intercettazioni, accesso ai dati personali e valori costituzionali*, Processi e Procedimenti, Pacini Giuridica, 2021, p. 26.
[274]Corte eur. 23 novembre 1993, *A. c. Francia*.

protezione del diritto alla vita privata. La conseguenza primaria di questa impostazione accomuna le due discipline, in quanto anche l'intercettazione di conversazioni rappresenta una grave ingerenza, da parte dello Stato e dei poteri pubblici, nel diritto alla vita privata, per cui è necessaria una normativa precisa, chiara ed esaustiva. Qualora la disciplina non presenti le necessarie garanzie derivanti dal rispetto dei diritti a tutela dell'individuo, si configurerebbe una violazione dell'art. 8 CEDU. È stato precisato dalla dottrina[275] come l'art. 15 Cost., in relazione alla disciplina delle intercettazioni, abbia lo scopo di proteggere e tutelare non tanto la riservatezza dei contenuti, bensì la segretezza delle comunicazioni, in quanto massima espressione dell'individuo.

Un ulteriore punto in comune con la disciplina della "*data retention*" riguarda la sanzione dell'inutilizzabilità, prevista all'art. 191 c.p.p. Su questo punto si sono espresse le Sezioni Unite affermando che l'inutilizzabilità dei risultati delle intercettazioni si configura nei casi previsti e disciplinati all'art. 271 c.p.p. e in tutti i casi di violazione delle prescrizioni previste agli artt. 267 e 268 c.p.p. Anche in questo caso, l'inutilizzabilità si presenta come una sanzione a presidio delle libertà e della segretezza delle comunicazioni, con conseguente totale eliminazione del materiale probatorio derivante dalle intercettazioni illegittime[276]. Inoltre, la Cassazione ha da sempre ritenuto applicabile alla disciplina delle intercettazioni, l'inutilizzabilità derivante dalle cosiddette "prove incostituzionali", in quanto prove ottenute mediante violazione di precetti costituzionali. La Suprema Corte ha specificato[277] come la patologia che affligge queste prove sia irreversibile e che non è necessario che le garanzie siano espressamente previste nei testi normativi, in

[275] P. FELICIONI, *Le fattispecie "atipiche" e l'impiego processuale*, in T. BENE (a cura di), *L'intercettazione di comunicazione*, Giustizia penale della post-modernità, Cacucci *Editore*, 2018, p. 321. A. CAPONE, *Intercettazione e Costituzione: problemi vecchi e nuovi,* in *Cass. pen.*, 2017, p. 1265, ed anche F. CAPRIOLI, *Colloqui riservati e prova penale,* Giappichelli, Torino, 2000, p. 11 e ss.

[276] Cass., Sez. Un., 13 gennaio 2009, n. 1153. In questa sentenza, la Suprema Corte afferma anche che l'inutilizzabilità dei risultati delle intercettazioni sollevata e dichiarata in un giudizio penale, ha conseguenze anche in giudizi promossi per la riparazione per ingiusta detenzione.

[277] Cass., Sez. Un., 23 febbraio 2000, n. 6.

quanto possono essere ricavate o da altre norme o dai principi generali previste dalla Costituzione.

È necessario soffermarsi anche sulla natura giuridica delle intercettazioni e della "*data retention*". La dottrina prevalente afferma che "mentre le intercettazioni consentono di captare il contenuto della conversazione, la "*data retention*" ha invece per definizione ad oggetto i dati esterni alla stessa"[278]. Di conseguenza si ritiene che, da punto di vista della possibile gravità della lesione del diritto alla riservatezza, la "*data retention*" possa causare il rilevamento delle abitudini dei soggetti coinvolti in misura maggiore di una intercettazione, la quale può essere anche sporadica e di breve durata[279]. Questa conclusione, alla quale l'autrice si associa, è sorretta anche da un'altra differenza che intercorre tra le due tecniche investigative. Infatti, l'intercettazione viene disposta nei confronti di un solo individuo in relazione alla propria utenza telefonica o telematica, mentre la "*data retention*", come più volte affermato nel corso di questo elaborato, comporta non solo la conservazione dei dati del singolo soggetto interessato dall'indagine, ma anche dei dati appartenenti ad altri soggetti totalmente estranei all'indagine in corso, cagionando nei confronti di quest'ultimi una lesione alla *privacy*.

In questo quadro di principi costituzionali e di pronunce giurisprudenziali sovranazionali, si è inserita la delega parlamentare[280], la quale merita un'analisi in quanto delinea un costante riferimento ai principi delineati a livello europeo. È stata così predisposta una disciplina delle intercettazioni in un'ottica di completezza, garantendo l'importanza necessaria al diritto alla riservatezza e alla *privacy* anche

[278] Cit. R. FLOR-S. MARCOLINI, *Dalla* data retention *alle indagini ad alto contenuto tecnologico: la tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato*, Giappichelli, 2022, p. 42.
[279] Ne parla anche la Corte di Giustizia nella sentenza del 6 ottobre 2020, Quadrature du Net, C-511/18, C-512/18 e C-520/18, al par. 117.
[280] Prevista all'art. 1, commi 82, 83 e 84, lett. a), b), c), d) ed e) della legge 23 giugno 2017, n. 103.

dei soggetti coinvolti solo occasionalmente nelle indagini, senza diminuire l'efficacia e l'operatività di questo mezzo di ricerca della prova[281].

Nonostante il costante richiamo ai principi della Corte, il legislatore italiano ha enfatizzato il ruolo centrale delle intercettazioni come mezzo di ricerca della prova ritenuto "imprescindibile"[282] nel panorama investigativo italiano, andando così in controtendenza rispetto al filone interpretativo delineato dalla giurisprudenza europea. A prescindere da ciò, l'esigenza di rispetto del diritto alla riservatezza è stata disciplinata dal legislatore in linea con l'interpretazione maggioritaria europea, non limitandosi sono all'attività investigativa in senso stretto, ma riferendosi anche all'attività di *post* captazione, con lo scopo principale di evitare la fuga di notizie e la divulgazione di elementi considerati non utili e non necessari ai fini delle indagini.

Viene, inoltre, sottolineata anche l'importanza del controllo giudiziale avente lo scopo di analizzare la sussistenza di tutti i parametri necessari per la legittimità delle operazioni, per impedire la cosiddetta "*data over-collection*" che potrebbe generare negli individui quella paura di una costante sorveglianza da parte dello Stato[283].

Il bilanciamento tra tutela della *privacy* ed esigenze pubbliche di investigazione, così come delineato nella legge-delega, non è poi stato seguito dal Governo, il quale nel d. lgs. del 29 dicembre 2017, n. 216 mostra una scarsa affezione ai principi di procedure penale europea[284].

---

[281] Anche qui di richiama al necessario equilibrio tra esigenze processuali e rispetto dei diritti fondamentali.
[282] S. BUZZELLI, *Le nuove intercettazioni tra selettività arbitraria e ridimensionamento delle garanzie*, in *Riv. Dir. dei media*, 2018, p. 5.
[283] Parere del Garante della *privacy* del 18 settembre 2015, Segreto di Stato ed accesso agli archivi.
[284] Per un approfondimento, D. CURTOTTI, *La giurisprudenza europea*, in T. BENE (a cura di), *L'intercettazione di comunicazione,* Giustizia penale della post-modernità, Cacucci Editore, 2018, p. 25 e ss. A. CAPONE, *Intercettazione e Costituzione: problemi vecchi e nuovi,* in *Cass. pen.*, 2017, p. 1265, ed anche F. CAPRIOLI, *Colloqui riservati e prova penale,* Giappichelli, Torino, 2000, p. 26 e ss.

Come primo accostamento delle due discipline, si può concludere affermando che, come la disciplina della "*data retention*", anche le intercettazioni si basano sul medesimo sfondo costellato dagli stessi principi sia costituzionali che sovranazionali. Entrambi i mezzi di ricerca della prova sono costantemente sorvegliati sia dal mondo della politica, sia dalla dottrina, che dalla giurisprudenza, italiana ed europea, in virtù della loro possibile ingerenza nella *privacy* e nella riservatezza dei soggetti. Ad oggi, sia la disciplina della "*data retention*" sia la normativa in materia di intercettazioni è al centro del dibattito politico[285], il quale punta ad una riforma di entrambe, ritenuta necessaria, affinché l'Italia diventi uno dei paesi europei che pone la necessaria attenzione ad un diritto fondamentale dell'individuo, come la *privacy*.

3. 8 Ulteriore riflessione sul principio di proporzionalità tra "*data retention*" ed intercettazioni

Sempre in riferimento al confronto tra le due discipline non si può non riservare un dovuto spazio di riflessione al principio di proporzionalità. Esso si può definire come un principio che impone che ogni disposizione normativa adottata raggiunga gli obiettivi prefissati dalle autorità, garantendo al tempo stesso che vengano incisi nella misura minima possibile le libertà, i diritti e gli interessi, a cui la misura fa riferimento[286].

In relazione alla disciplina della "*data retention*", un'importante riflessione giurisprudenziale sul tema della proporzionalità si è avuto a seguito della sentenza

[285] Attualmente la Riforma Nordio è all'esame della commissione Giustizia al Senato, la cui Presidente, Giulia Buongiorno, ha sottolineato come questo riforma punti alla tutela della *privacy* soprattutto di quei soggetti che non centrano con le indagini.

[286] Per approfondimento, G. TABASCO, *Principio di proporzionalità e misure cautelari*, Cedam, 2017. E anche P. FELICIONI, *Le fattispecie "atipiche" e l'impiego processuale*, in T. BENE (a cura di), *L'intercettazione di comunicazione*, Giustizia penale della post-modernità, Cacucci Editore, 2018, p. 303.

della Corte di Giustizia sul caso "*Digital Rights Ireland*"[287] con la quale è stata dichiarata invalida la Direttiva Frattini appunto per mancanza di proporzionalità[288].

È opportuno esaminare un'ulteriore vicenda che ha consentito alla Corte di Giustizia di statuire nuovamente sul ruolo del principio di proporzionalità e di precisare la portata dei principi già delineati nel 2014: la sentenza del 2 ottobre 2018 della Corte di Giustizia denominata "*Ministero Fiscal*"[289]. La vicenda trae origine da un caso spagnolo, il quale riguardava un episodio di "*robo con violencia*"[290] del portafoglio e del cellulare, in relazione al quale la polizia giudiziale spagnola aveva chiesto al giudice istruttore di essere autorizzata ad avanzare richiesta a tutti i fornitori di servizi di comunicazione, al fine di venire a sapere se con il codice IMEI[291] del telefono oggetto della rapina fosse stata attivata una nuova SIM. L'intento investigativo della polizia giudiziaria era chiaro: se il rapinatore avesse tolto la SIM precedente ed originaria inserendone una nuova, sarebbe stato possibile individuare i dati indentificativi dell'intestatario di questa nuova SIM. In seguito però, il giudice istruttore spagnolo ha negato l'autorizzazione. Di conseguenza il Pubblico Ministero ha impugnato questa decisione. Successivamente il giudice dell'impugnazione prima di decidere, sospende il giudizio e rinvia pregiudizialmente alla Corte di Giustizia.

Per la Corte questa è un'altra occasione per tornare ad affermare la delicatezza della disciplina della "*data retention*", la quale consente di conoscere tutta una serie di elementi "sulla vita privata delle persone i cui dati sono oggetto di attenzione"[292]. E inoltre ribadisce che la "*data retention*" può causare una seria lesione del diritto

[287] Corte giust. UE, 8 aprile 2014, "*Digital Rights Ireland*", cause riunite C-293/12 e C-594/12.
[288] Si rinvia al paragrafo 1.6 per approfondimento.
[289] Corte giust. UE, 2 ottobre 2018, "*Ministero Fiscal*", C-207/16.
[290] In Italia parleremo di rapina ex art. 628 c.p.
[291] Il codice IMEI deriva dall'inglese *International Mobile Equipment Identity* ed è un codice numerico di 15 cifre, divisa in 4 differenti sezioni delimitate da trattini e univoco per ogni dispositivo. Esso consente l'identificazione del dispositivo da parte della rete telefonica, in quanto non può essere copiato o ereditato da altri terminali.
[292] Corte giust. UE, 2 ottobre 2018, "*Ministero Fiscal*", C-207/16, par 60.

alla riservatezza, ma "tale lesione viene consentita, in virtù del principio di proporzionalità, sono nel contesto delle indagini per i reati più gravi"[293].

La novità prospettata da questa sentenza riguarda la possibilità di individuare lesioni al diritto alla *privacy* sempre e comunque rilevanti, ma definite "meno gravi"[294], come appunto il caso in esame dove si cercava di individuare un collegamento tra un dispositivo e il suo codice IMEI, con una nuova SIM e il suo intestatario. La Corte sostiene obiettivamente l'esistenza di un possibile attacco alla riservatezza e una possibile lesione del diritto alla *privacy*, ma lo definisce più lieve[295], in quanto il principio di proporzionalità, in questo caso, consente un bilanciamento tra beni giuridici normalmente in conflitto. In questa impostazione della Corte, si assiste ad una modulazione graduata e variabile del principio di proporzionalità sempre rapportato principalmente alla lesione del diritto alla riservatezza, ma configurando differenti gradi di protezione del bene giuridico della *privacy* a seconda che l'intervento delle autorità pubbliche, per mezzo della *"data retention*", si configuri come più o meno gravoso per la riservatezza e la *privacy* dell'individuo.

Anche in relazione alla disciplina delle intercettazioni, il principio di proporzionalità assume un ruolo centrale. Viene in considerazione la portata applicativa più ampia del principio stesso, ovvero il concetto per cui la proporzionalità è vista, dalla maggior parte della dottrina sia italiana che europea, come criterio di controllo delle limitazioni ai diritti fondamentali, in questo caso *privacy* e riservatezza, imposte dallo Stato e dalle Autorità pubbliche. È opportuno ricomprendere anche le intercettazioni nella portata normativa dell'art. 8 CEDU, in

[293] Corte giust. UE, 2 ottobre 2018, "*Ministero Fiscal",* C-207/16, par 56: "in conformità al principio di proporzionalità, infatti, una grave ingerenza può essere giustificata, in materia di prevenzione, ricerca, accertamento e perseguimento di un reato, solo da un obiettivo di lotta contro la criminalità che deve essere qualificata come grave".

[294] Cit. R. FLOR-S. MARCOLINI, *Dalla* data retention *alle indagini ad alto contenuto tecnologico: la tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato*, Giappichelli, 2022, p. 17.

[295] Corte giust. UE, 2 ottobre 2018, *"Ministero Fiscal*", C-207/16, par 61: "l'accesso ai soli dati oggetto della domanda di cui trattasi nel procedimento principale non può essere qualificato come un'ingerenza grave nei diritti fondamentali delle persone i cui dati sono oggetto di attenzione."

quanto uno strumento investigativo che possa comprimere il diritto alla *privacy* o alla riservatezza deve essere utilizzato con lo scopo di raggiungere una delle finalità legittimamente previste da una (necessaria) disposizione normativa, in modo tale da giustificare un eventuale ingerenza come proporzionata[296].

Di conseguenza le Corti europee si sono espresse, sin da tempo, in merito al principio di proporzionalità anche in riferimento alla disciplina delle intercettazioni, affermando che il suddetto principio stabilisce quelle che sono le limitazioni e i casi di ammissibilità di una tecnica investigativa così invasiva nei diritti fondamentali. In più, la Corte Europea dei Diritti dell'Uomo fa costantemente riferimento ad un'attività di controllo "effettivo" circa il perseguimento degli obiettivi tramite un'attività investigativa rispettosa dei diritti fondamentali[297], in modo tale da scongiurare il pericolo di azioni di controllo dei cittadini da parte dello Stato[298].

In conclusione, lo scopo del confronto tra le due discipline è il seguente: nonostante le differenze strutturali e procedurali[299] dei due mezzi di ricerca della prova, si è voluto sottolineare la persistenza dei medesimi principi costituzionali e sovranazionali a tutela della riservatezza e della *privacy*, i quali continuano ad "orientare" le interpretazioni delle Corti europee. A sua volta, le Corti spingono i singoli Stati ad adottare discipline complete, chiare ed efficienti dal punto di vista

---

[296] Così, P. FELICIONI, *Le fattispecie "atipiche" e l'impiego processuale*, in T. BENE (a cura di), *L'intercettazione di comunicazione*, Giustizia penale della post-modernità, Cacucci Editore, 2018, p. 329.

[297] Corte eur., Sez. IV, 29 marzo 2005, *Matheron c. Francia.*

[298] Ribadito anche da L. FILIPPI, *Intercettazioni, accesso ai dati personali e valori costituzionali*, Processi e Procedimenti*,* Pacini Giuridica, 2021, p. 30. Vengono citate le condizioni per la legittimità di una procedura di intercettazioni individuate dalla Corte Europea dei Diritti dell'Uomo. Per citarne alcune: esistenza di un'ingerenza; giustificazione dell'ingerenza; natura dei crimini; categoria delle persone oggetto delle intercettazioni; durata delle intercettazioni telefoniche; …
Sul punto anche, Corte eur., 10 marzo 2009, *Bykov c. Russia,* in cui la Corte accertò la violazione dell'art. 8 CEDU in un caso di intercettazione e registrazione di una conversazione mediante un apparecchio di radiotrasmissione nell'ambito di un'operazione segreta di polizia, condotta quindi senza garanzie processuali.

[299] Per quanto concerne la disciplina delle intercettazioni, L. FILIPPI, *Intercettazioni, accesso ai dati personali e valori costituzionali*, Processi e Procedimenti*,* Pacini Giuridica, 2021. Mentre per un approfondimento ulteriore sulla disciplina della "*data retention*", R. FLOR-S. MARCOLINI, *Dalla* data retention *alle indagini ad alto contenuto tecnologico: la tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato*, Giappichelli, 2022.

operativo, servendosi sempre del principio di proporzionalità come principale "linea guida".

3. 9 Le tipologie di dati interessati dalla "*data retention*" e il problema della base giuridica all'indomani della sentenza della Corte di Giustizia "*Digital Rights Ireland"*

È necessario trattare anche di una questione più tecnica, ma indispensabile per concludere questo *excursus* sulla disciplina della "*data retention*", ovvero i cosiddetti dati esterni alle comunicazioni.

Per dati esterni alle comunicazioni[300], interessati quindi dalla disciplina della "*data retention*", si intendono tutti i dati necessari al tracciamento e all'identificazione di una fonte di una comunicazione, quindi numero di telefono, i dati del soggetto abbonato ad un data compagnia telefonica, l'accesso ad *Internet*, gli indirizzi di posta elettronica e di messaggistica telematica. Vengono ricompresi inoltre anche quei dati che servono per rintracciare la destinazione di una comunicazione, identificando così il soggetto ricevente della stessa, per determinare l'ora, la durata e la data della comunicazione, come per esempio data e ora del *log-in* e *log-out* dal servizio di comunicazione telematica e l'indirizzo IP. Sempre a titolo esemplificativo, i dati di cui si parla sono anche quelli che consentono di determinare la natura della comunicazione o del servizio *Internet* utilizzato dal soggetto, in modo tale da eseguire una triangolazione geografica e identificare così l'ubicazione del dispositivo[301].

[300] Ulteriore approfondimento, M. RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico*, in *Dir. pen. cont.*, 2016.
[301] R. FLOR-S. MARCOLINI, *Dalla* data retention *alle indagini ad alto contenuto tecnologico: la tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato*, Giappichelli, 2022, p. 75.

In conclusione, si tratta di tutti i dati esterni alla comunicazione, che resta così segreta[302], i quali hanno enormi potenzialità in ambito investigativo e difensivo, in quanto di rilievo strategico e potenzialmente rivelatori di numerose ed importanti informazioni.

Nella pratica, quando un soggetto effettua una chiamata telefonica[303], questa genera dei dati, i quali possono rivelarsi utili nel caso di un'indagine o a fini difensivi nei confronti del soggetto che ha effettuato la chiamata. Tali dati, i dati relativi al traffico e i dati relativi all'ubicazione[304], vengono trattati dal gestore della compagnia, il quale li conserva nella misura necessaria al perseguimento dei reati per cui è prevista la disciplina della *"data retention"*, con conseguente adozione da parte dei gestori delle misure tecniche ed organizzative necessarie che permettano la conservazione di un numero importante di dati per un periodo di tempo che, come già visto, è di 6 anni. Lo scopo delle misure adottate dal gestore è quello di assicurare livelli di sicurezza tali da evitare possibili abusi e accessi illeciti[305].

A seguito della sentenza "*Digital Rights Ireland*" della Corte di Giustizia, con la quale è stata dichiarata l'invalidità della Direttiva "Frattini", la base giuridica della disciplina della "*data retention*" è nuovamente la Direttiva 2002/58/CE, disciplina ritenuta comunque eccessivamente generica in relazione allo scopo principale di armonizzazione delle discipline degli Stati Membri.

In merito a questa situazione di possibile *vacuum* normativo, la Corte di Giustizia si è espressa sulla questione[306], ancora aperta, dei rapporti intercorrenti tra le

[302] La captazione del contenuto della comunicazione, è compresa nell'operatività della disciplina delle intercettazioni.
[303] Definita meglio come "comunicazione elettronica", della quale la Direttiva 2002/58/CE all'art. 2, par. 1, lett d) ci fornisce la definizione: "ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono esclude le informazioni trasmesse, come parte di un servizio di radiodiffusione, al pubblico tramite una rete di comunicazioni elettronica salvo quando le informazioni possono essere collegate all'abbonato o utente che riceve le informazioni che può essere identificato".
[304] Entrambi previsti nella Direttiva 2002/58/CE e trasposti nell'art. 121 codice *privacy*.
[305] Aspetto, quello della sicurezza del trattamento, previsto dalla Direttiva 2002/58/CE all'art. 4.
[306] Corte giust. UE, 21 dicembre 2016, *Tele2 Sverige e Watson*, cause riunite C-203/15 e C-698/15. Si tratta appunto di due domande pregiudiziali, successivamente riunite: la prima riguardava un caso

discipline nazionali e il diritto comunitario in relazione alla "*data retention*". La questione principale decisa dalla Corte riguarda la collocazione euro-unitaria della "*data retention*" a seguito dell'annullamento della Direttiva "Frattini". La Corte, nella sua motivazione, rivela la sua posizione rispetto alle molteplici opinioni espresse dai singoli Stati, statuendo che le disposizioni nazionali in tema di "*data retention*", riguardanti la conservazione dei dati e l'accesso ai medesimi da parte delle pubbliche autorità, ricadono nuovamente all'interno dell'ambito di operatività della Direttiva 2002/58/CE[307].

In relazione alle categorie di dati esterni alle comunicazioni indicate dalla Direttiva "Frattini" all'art. 5, la Corte ha specificato che da un punto di vista prettamente tecnico l'elencazione inizialmente prevista dalla Direttiva invalidata viene tutt'oggi intesa come punto di riferimento ancora valido. Di conseguenza, si potrà applicare la disciplina della conservazione e dell'accesso con successiva ed eventuale acquisizione di quelle categorie di dati precedentemente indicati nella Direttiva "Frattini" in quando attualmente ancora validi.

In aggiunta alla Direttiva 2002/58/CE, un'ulteriore base giuridica della "*data retention*" può essere ravvisata nella Direttiva 2016/680/UE, in attesa dell'intervento del legislatore mediante un nuovo provvedimento. La presente Direttiva concerne la protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione dei suddetti dati. L'accostamento della Direttiva alla disciplina della "*data retention*" è data dal fatto che la stessa Direttiva, tra i suoi principi generali, indica il principio di proporzionalità come prescrizione generale in relazione all'attività di trattamento dei dati, in quanto "i dati personali siano

svedese promosso dalla società *Tele 2 Sverige AB* contro *l'authority* svedese in materia di poste e telecomunicazioni; la seconda causa concerne un giudizio inglese, promosso da 3 cittadini contro il Ministero dell'Interno britannico.

[307] Corte giust. UE, 21 dicembre 2016, *Tele2 Sverige*, cause riunite C-203/15 e C-698/15, parr. 65 e ss.

adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono trattati"[308]. Vi sono altri numerosi riferimenti, all'interno della Direttiva, in relazione alle indicazioni giurisprudenziali fornite in tema di "*data retention*", come: i termini per la cancellazione dei dati personali; la predisposizione di misure procedurali; la chiara distinzione, da parte del titolare del trattamento, tra i dati personali delle diverse categorie di soggetti interessati, con diversificazione in base al rapporto intercorrente tra il soggetto e il reato per cui si procede[309]. Nonostante il parere favorevole del Garante della *privacy*[310] espresso in relazione a suddetta Direttiva, questa impostazione provvisoria resta frutto del pensiero dottrinale, al quale l'autrice si associa, in quando il legislatore resta tutt'ora silente.

Attualmente la dottrina ritiene che la sentenza della Corte sul caso "*Digital Rights Ireland*" costituisca il primo passo per delineare uno "statuto"[311] di regole unitario della disciplina della "*data retention*", con specificazione degli elementi reputati indispensabili[312] a cui il legislatore deve dare assoluta importanza.

In conclusione, al termine di questo *excursus* sulla disciplina della "*data retention*", molteplici sono le problematiche ancora aperte in quanto sia il legislatore nazionale sia, *in primis*, quello euro-unitario, non siano ancora intervenuti, al fine di introdurre una nuova normativa, ovvero una completa base giuridica.

---

[308] Art. 4 Direttiva 2016/680/UE.
[309] Ne parla anche M. IASELLI*, Dati giudiziari in ambito penale: recepita la direttiva europea*, in *Altalex*, 2018.
[310] Parere del Garante della *privacy* sullo schema di decreto legislativo recante Attuazione della Direttiva 2016/680/UE del Parlamento europeo e del Consiglio, 22 febbraio 2018.
[311] Cit. R. FLOR-S. MARCOLINI, *Dalla* data retention *alle indagini ad alto contenuto tecnologico: la tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato*, Giappichelli, 2022, p. 11.
[312] Per esempio, la specificazione dei gravi reati, i casi e modi di accesso al dato da parte dell'autorità, il periodo di conservazione e la sicurezza dei dati conservati.

Conclusioni

Il presente elaborato si è posto l'intento di esaminare la disciplina della "*data retention*", dall'introduzione del concetto di *privacy* fino agli ultimi interventi legislativi, europei e nazionali, e alle ultime interpretazioni giurisprudenziali.

Sulla base dei risultati illustrati, potrebbero prospettarsi due scenari distinti. Da un lato, i legislatori, sovranazionali e nazionali, potrebbero adottare una serie di decisioni innovative dando così vita ad una ulteriore riforma, questa volta onnicomprensiva, che intervenga sui diversi fronti ancora problematici dell'art. 132 codice *privacy* e della disciplina della "*data retention*". Sarà necessario avviare un nuovo dibattito giurisprudenziale e dottrinale sulla disciplina interna, nel quale anche le stesse Corti nazionali rivestiranno un ruolo importante orientando il legislatore verso decisioni più consapevoli della propria portata e delle proprie conseguenze sulla disciplina interna. L'altro scenario, per certi versi negativo, che potrebbe verificarsi tenderebbe ad una conferma di quanto stabilito fino ad ora sia dalla giurisprudenza europea sia dal legislatore interno, generando così un immobilismo normativo e un mancato intervento su questioni problematiche della disciplina.

È ancora presto per trarre un bilancio positivo o negativo dell'ultimo intervento riformistico. Le criticità tutt'oggi presenti nella disciplina non sono solo questioni di natura meramente tecnica: si intende ricordare le problematiche della disciplina transitoria, legate ad una sua originaria previsione nel testo normativo, con successiva rimozione, per poi essere reintrodotta nella legge di conversione, con le relative criticità interpretative; la questione del controllo preventivo del giudice, forse il profilo più discusso della riforma; ed infine il criterio della gravità del reato, criterio presupposto per l'applicazione della disciplina riformata, che resta un punto dubbioso anche alla luce delle recenti interpretazioni della Corte di Giustizia dell'Unione Europea.

Inoltre, resta ancora aperto il fronte delle tempistiche di conservazione dei dati, non ancora interessato da un intervento riformistico, nonostante il parere del Garante per la protezione dei dati personali e di numerosi esperti che, da tempo, tentano di riportare l'attenzione del legislatore su questo importante e delicato aspetto.

Sarà compito del legislatore chiarire la complessa, ma considerevole, questione concernente il necessario equilibrio tra esigenze di sicurezza nazionale e il diritto fondamentale alla *privacy* al fine di scongiurare quel rischio di incontrollata e indeterminata vigilanza sui cittadini. Sarà appropriato concentrarsi su una disciplina che compensi, da un lato, le esigenze di repressione dei reati e di sicurezza nazionale e, dall'altro, la salvaguardia dei diritti fondamentali, con riferimento in questo caso alla *privacy*.

In definitiva, si può affermare come la disciplina interna della "*data retention*" sia interessata da tante critiche quante incertezze che attengono sia al profilo della conservazione dei dati di traffico telefonico e telematico sia alla relativa procedura di acquisizione degli stessi per scopi investigativi e di contrasto a forme di criminalità rilevanti per la sicurezza nazionale.

Ad oggi, il futuro approccio legislativo e giurisprudenziale interno è di difficile previsione. Non si discute sulla delicatezza della disciplina della "*data retention*", perciò è necessario individuare e stabilire le adeguate tutele e i necessari limiti della stessa.

Al momento, quindi, la "strada" riformistica è senza dubbio necessaria quanto delicata e complicata, anche tenendo conto dell'innovazione tecnologica, elemento essenziale della disciplina.

In conclusione, dunque, l'elaborato si allinea a tutti quegli scritti di autorevoli esperti, i quali sostengono l'inadeguatezza dell'odierna disciplina ed auspicano un intervento riformistico che sia consapevole della delicatezza e dell'importanza dei diritti coinvolti.

Bibliografia

AGENZIA EUROPEA PER I DIRITTI FONDAMENTALI, *Data retention across the EU*, luglio 2017.

ALBANESE D., *La corte di cassazione sulla legittimità della disposizione transitoria relativa alla nuova disciplina in materia di* data retention, in *Sistema Penale*, aprile 2022.

ALBANESE D., *Dalla Corte di giustizia dell'Unione europea un'altra svolta garantista in materia di acquisizione dei tabulati telefonici*, in *Sistema Penale*, maggio 2024.

ALESCI T.-BENE T.-BUONOMO G.-CAPRIOLI F.-CURTOTTI D.-DI BITONTO M. L.-DI GERONIMO P.-FELICIONI P.-GALANTINI N.-GIORDANO L.-GRASSIA R. G.-IASEVOLI C.-MAGGIO P.-NOCERA A.-PILLA E.-RUGGERI F.-VERGINE F., *L'intercettazione di comunicazione*, in T. BENE (a cura di), in *Giustizia penale della post-modernità*, Caucci Editore, 2018.

AMATO G., *Nella "costruzione" normativa si è sminuito il ruolo del Pm*, in *Guida al diritto*, 2021.

ANDOLINA E., *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, Wolters Kluver-Cedam, 2018.

BANFI F., *Quali sono i reati informatici più diffusi? I reati informatici più diffusi: alcune statistiche*, in *Diritto Consenso*, aprile 2023.

BATTARINO G., *Acquisizione di dati di traffico telefonico e telematico per fini di indagine penale: il decreto-legge 30 settembre 2021, n. 132*, in *Questione giustizia*, 2021.

BORGOBELLO M., *Acquisizione di tabulati telefonici: che cosa cambia col nuovo decreto-legge*, in *Agenda Digitale*, 2021.

BRANDEIS L.-WARREN S., *The right to* privacy, in *Harvard Law Review*, dicembre 1890.

BUCCI F., Data retention*: stato dell'arte e sviluppi recenti in Europa*, in *Ius Itinere*, 2020.

BUFFA M., "Data retention" *e diritto transitorio: un possibile punto fermo giurisprudenziale*, in *Questione Giustizia*, 2022.

BUZZELLI S., *Le nuove intercettazioni tra selettività arbitraria e ridimensionamento delle garanzie*, in *Riv. Dir. dei media*, 2018.

CAGGIANO G., *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*, in *Nuove Tecnologie e Diritti Umani*, *Saggi*, 2017.

CAMON A., *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Riv. Proc. Pen*., 2005.

CAPONE A., *Intercettazione e Costituzione: problemi vecchi e nuovi*, in *Cass. Penale*, 2017.

CAPRIOLI F., *Colloqui riservati e prova penale*, Giappichelli, Torino, 2000.

CARDONE A., *Il sistema della* Data Retention *come strumento investigativo*, in *Giurisprudenza Penale*, 2021.

CHINNICI D., *L'inutilizzabilità della prova, tra punti fermi e profili controversi*, in *Diritto Penale e Processo*, luglio 2014.

CISTERNA A., *Attuazione della Dir. 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la Dir. 2002/58/CE (commento al d. leg. 30 maggio 2018, n. 109)*, in *Guida al Diritto*, 2008.

COLAPIETRO C., *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *federalismi.it*, *Riv. Dir. Pub.*, 2018.

COMMISSIONE EUROPEA, *Relazione COM (2003) 265 sull'applicazione della direttiva sulla tutela dei dati (95/46/CE),* Bruxelles, 15 maggio 2003.

COMMISSIONE EUROPEA, *Relazione COM (2011) 225 definitivo sulla valutazione dell'applicazione della direttiva sulla conservazione dei dati (direttiva 2006/24/CE)*, Bruxelles, aprile 2011.

CONTI C., *Accertamento del fatto e inutilizzabilità nel processo penale*, Cedam, 2007.

DALLA TORRE J., *L'acquisizione dei tabulati telefonici nel processo penale dopo la sentenza della Grande Camera della Corte di Giustizia UE: la svolta garantista in un primo provvedimento del g.i.p. di Roma*, in *Sistema Penale*, 2021.

DE SALVIA M., *Dati personali e sfera privata nella giurisprudenza della Corte europea dei diritti dell'uomo: ricostruzione sommaria delle linee-guida*, in (a cura di) M. FUMAGALLI MERAVIGLIA, *Diritto alla riservatezza e progresso tecnologico. Coesistenza pacifica o scontro di civiltà?,* Editoriale scientifica, 2015.

DE SIMONE P. E., *La rilevanza probatoria dei tabulati telefonici comprovanti la localizzazione di un'utenza telefonica (c.d. "pedinamento elettronico")*, in *Jus*, aprile 2023.

FERRUA P., *La ragionevole durata del processo tra Costituzione e Convenzione europea*, in *Questione Giustizia*, 2017.

FERRUA P., *Ammissibilità della prova e divieti probatori*, in *Revista Brasileira de Direito Processual Penal*, 2021.

FILIPPI L., *La Grande Camera della Corte di giustizia U.E boccia la disciplina italiana sui tabulati*, in *Penale. Diritto e Procedura*, 2021.

FILIPPI L., *La nuova disciplina dei tabulati: il commento "a caldo" del Prof. Filippi*, in *Penale. Diritto e Procedura*, 2021.

FILIPPI L., *Intercettazioni, acceso ai dati personali e valori costituzionali*, in *Processi e Procedimenti*, Pacini Giuridica, 2021.

FIORUCCI G., *Disorientamenti applicativi in tema di inutilizzabilità e tutela sostanziale del contraddittorio*, in *Archivio Penale*, settembre-dicembre 2022.

FLOR R.-MARCOLINI S., *Dalla* data retention *alle indagini ad alto contenuto tecnologico, La tutela dei diritti fondamentali quale limite al potere coercitivo dello Stato, Aspetti di diritto penale processuale e sostanziale*, Giappichelli, 2022.

FORMICI G., *Tutela della riservatezza delle comunicazioni elettroniche: riflessioni (ri)partendo dalla pronuncia* Ministero Fiscal, in *Osservatorio Costituzionale*, 2018.

FORMICI G., *La direzione indicata dalle Conclusioni dell'Avvocato Generale* Collins *nel caso C-178/22*, in *Media Laws*, 2022.

FORMICI G., "The three Ghosts of data retention*": passato, presente e futuro della disciplina italiana in materia di conservazione e acquisizione dei metadati per scopi investigativi. Commento a margine del d. l. 30 settembre 2021, n. 132 e relativa legge di conversione*, in *Osservatorio Costituzionale*, 2023.

FROSINA P., *La nuova legge sui tabulati telefonici non tutela la* privacy *ma rallenta inchieste e processi. E su alcuni reati sarà più difficile indagare*, in "*Il Fatto Quotidiano"*, 2021.

GALANTINI N., *L'inutilizzabilità della prova nel processo penale*, in *Pubblicazione del Dipartimento di Scienze Giuridiche dell'Università di Trento*, Cedam, 1992.

GARANTE DELLA PRIVACY, *Parere sull'accesso ai dati telefonici: garanzie per le chiamate in entrata*, 3 novembre 2005.

GARANTE DELLA PRIVACY, *Parere 2/2006 sugli aspetti di tutela della vita privata inerenti ai servizi di screening dei messaggi di posta elettronica*, 21 febbraio 2006.

GARANTE DELLA PRIVACY, *Provvedimento sulla sicurezza dei dati di traffico telefonico e telematico*, 17 gennaio 2008.

GARANTE DELLA PRIVACY, *Parere 2/2008 sul riesame della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche*, 15 maggio 2008.

GARANTE DELLA PRIVACY, *Parere sul segreto di Stato ed accesso agli archivi*, 18 settembre 2015.

GARANTE DELLA PRIVACY, *Parere sullo schema di decreto legislativo recante Attuazione della Direttiva 2016/680/UE del Parlamento europeo e del Consiglio*, 22 febbraio 2018.

GARANTE DELLA PRIVACY, *Parere 310/2021 sullo schema del decreto-legge per la riforma della disciplina di acquisizione dei dati relativi al traffico telefonico e telematico a fini di indagine penale*, 10 settembre 2021.

GARANTE DELLA PRIVACY, *Relazione annuale 2021*, presentata al Senato il 7 luglio 2022.

GATTA G. L., *Lentezza dei processi e giustizia penale come tela di Penelope*, in "*Sole 24 Ore*", 2023.

GITTARDI C., *Sull'utilizzabilità dei dati del traffico telefonico e telematico acquisiti nell'ambito dei procedimenti pendenti alla data del 30 settembre 2021*, in *Giustizia Insieme*, 2021.

GRANGER M. P.-IRION K., *The right to the protection of personal data: the new posterchild of European Union citizenship?*, in *Civil Rights and EU Citizenship*, Cheltenham, 2018.

GRIFANTINI F. M., *Il segreto difensivo nel processo penale*, Giappichelli, 2001.

IASELLI M., *Dati giudiziari in ambito penale: recepita la direttiva europea*, in *Altalex*, 2018.

ILLUMINATI G.-GIULIANI L., *Commentario breve al codice di procedura penale, Terzo Libro, Titolo I*, Cedam, 2020.

MAGNUSSON SJONBERG C., *Threats to personal data security: how does the EU protect its citizens?*, in *The European Union*, Cheltenham, 2018.

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

MALACARNE A.-TESSITORE G., *La ricostruzione della normativa in tema di* data retention *e l'ennesima scossa della corte di giustizia: ancora inadeguata la disciplina interna?*, in *Archivio Penale*, 2022.

MARCOLINI S., *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen*., 2015.

MIRANDA R., *Gli obblighi del gestore: esigenze di* data protection *o di* data retention?, in *Mezzi di Comunicazione e Riservatezza*, Jovene, 2008.

NATALINI A., *Misure urgenti in tema di acquisizione dei dati relativi al traffico telefonico e telematico a fini di indagine penale (art. 1 d. l. 30 settembre 2021, n. 132),* in *Ufficio del Massimario e del Ruolo, Servizio Penale, Rel. N. 55/2021,* in ACIERNO M.-ANDREAZZA G. (a cura di), in *Cass. pen.,* ottobre 2021.

OBERTO E., *L'inutilizzabilità della prova nel processo penale*, in *Ius Itinere*, maggio 2019.

PARODI C., *Tabulati telefonici: la Suprema Corte si esprime dopo le indicazioni della CGUE*, in *Ilpenalista.it*, 2021.

PESTELLI G., *D. L. 132/2021: un discutibile e inutile aggravio di procedura per tabulati telefonici e telematici*, in *Altalex*, 2021.

PESTELLI G., *Convertito in legge il D. L. 132/2021: le modifiche apportate (e quelle mancate) in materia di tabulati*, in *Altalex*, 2021.

PIZZETTI F., *Le sfide della nuova* privacy *nella società digitale e dell'IA*, in *Agenda Digitale*, 2023.

POLLICINO O.-BASSINI M., *La Corte di giustizia e una trama ormai nota: la sentenza* Tele2 Sverige *sulla conservazione dei dati di traffico per finalità di sicurezza e di ordine pubblico*, in *Dir. pen. cont.*, 2016.

POLLICINO O.-BASSINI M., *Commento all'art. 8 CdfUE*, in (a cura di) R. MATROIANNI-O. POLLICINO-S. ALLEGREZZA-F. PAPPALARDO-O. RAZZOLINI, *Carta dei diritti fondamentali dell'Unione Europea*, Giuffrè, 2017.

RECCHIA C.-SCORZELLI F., Privacy: *il nuovo pacchetto di normativa europea per la protezione dei dati personali*, in *Annunziata&conso*, 2017.

RICCARDI M., *Dati esteriori delle comunicazioni e tabulati di traffico,* in *Dir. pen. cont.*, 2016.

ROSSI DAL POZZO F., *La tutela dei dati personali nella giurisprudenza della Corte di giustizia*, in *Eurojus*, 2018.

SCACCIA G., *Corte costituzionale e doppia pregiudizialità: la priorità del giudizio incidentale oltre la Carta dei diritti?,* in *Quaderni Costituzionali*, *Riv*., 2020.

SCAGLIARINI S., *La Corte di Giustizia bilancia diritto alla vita privata e lotta alla criminalità: alcuni pro e alcuni contra*, in *Il Diritto dell'Informazione e dell'Informatica*, 2014.

SCAGLIARINI S., *La tutela della* privacy *e dell'identità personale nel quadro dell'evoluzione tecnologica*, in *Consulta Online*, 2021.

SCARCELLA A., *Geolocalizzazione: no all'utilizzabilità dei tabulati se manca l'autorizzazione*, in *Il Quotidiano Giuridico*, aprile 2023.

SCERBO N., *L'importanza dei dati e la loro gestione da parte dell'autorità*, in *Altalex*, 2023.

SIGNORATO S., *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.

SIRACUSANO D.-SIRACUSANO F., *Le prove*, in DI CHIARA G.-PATANÈ V.-SIRACUSANO F. (a cura di), in *Diritto processuale penale*, Giuffrè, 2018.

TABASCO G., *Principio di proporzionalità e misure cautelari*, Cedam, 2017.

TONDI V., *La disciplina italiana in materia di* data retention *a seguito della sentenza della Corte di giustizia UE*, in *Sistema Penale*, 2021.

TONINI V. P., *Il valore probatorio dei documenti contenenti dichiarazioni scritte*, in *Cass. pen.*, 1990.

TRONCONE P., *Profili penali del codice della* privacy, in *Riv. pen.*, 2004.

VADAPALAS V., *Legal Opinion*, 2022.

VECCHIO F., *L'ingloriosa fine della direttiva* Data retention*, la ritrovata vocazione costituzionale della Corte di Giustizia e il destino dell'art. 132 Codice della* privacy, in *Rivista Elettronica del Centro di Documentazione Europea dell'Università Kore di Enna*, 2014.

VIGGIANO M*., Navigazione in* Internet *e acquisizione occulta dei dati personali*, in *Il Diritto dell'Informazione e dell'Informatica*, 2007.

VITIELLO M., *Celle telefoniche e tabulati: cosa sono e come vengono analizzati nei casi giudiziari*, in *Cybersecurity 360*, 2022.

Indice delle pronunce

Griswold vs *Connecticut*, 7 giugno 1965.

Corte cost., 4 aprile 1973, n. 34.

Corte cost., 12 aprile 1973, n. 38.

Corte cost., 11 marzo 1993, n. 81.

Corte eur., 23 novembre 1993, *A. c. Francia*.

Corte eur., 30 luglio 1998, *Venezuela Contreras c. Spagna*.

Corte eur., 16 febbraio 2000*, Amann c. Svizzera*

Cass. pen., Sez. Un., 23 febbraio 2000, n. 6.

Corte cost., 6 luglio 2001, n. 224.

Corte eur., Sezione IV, 29 marzo 2005, *Matheron c. Francia.*

Cass. pen., Sez. VI, 4 maggio 2006, n. 33435.

Cass. pen., Sez. Un., 13 gennaio 2009, n. 1153.

Corte eur., 10 marzo 2009, *Bykov c. Russia.*

Cass. pen., Sez. Un., 23 aprile 2009, n. 23868.

Cass. pen., Sez. Un., 16 luglio 2009, n. 39061.

Corte cost., 16 febbraio 2012, n. 22.

Corte eur., 30 aprile 2013, *Cariello e altri c. Italia.*

Corte cost., 9 luglio 2013, n. 183.

Corte giust. UE, 8 aprile 2014, *Digital Rights Ireland*, cause riunite C-293/12 e C-594/12.

Cass. pen., Sez. V, 25 gennaio 2016, n. 7265.

Corte giust. UE, 21 dicembre 2016, *Tele 2 Sverige* e *Watson*, cause riunite C-203/15 e C-698/15.

Corte giust. UE, 2 ottobre 2018, *Ministero Fiscal*, C-207/16.

Corte cost. 3 ottobre 2019, n. 219.

Cass. pen., Sez. VI, 1° ottobre 2020, n. 37074.

Corte giust. UE, 6 ottobre 2020, *La Quadrature du Net* e *altri*, cause riunite C-511/18, C-512/18 e C-520/18.

Corte giust. UE, 2 marzo 2021, *H.K* v. *Prokuratuur*, C-746/18.

Cass. pen., Sez. II, 15 aprile 2021, n. 28523.

Conseil d'Etat, 21 aprile 2021*, French Data Network et al*., n. 393099, n. 394922, n. 397844, n. 397581, n. 424717, n. 424718.

Cass. pen., Sez. V, 13 gennaio 2022, n. 1054.

Cass. pen., Sez. III, 1° aprile 2022, n. 11993.

Corte giust. UE, Grande Sezione, 5 aprile 2022, "*Commissioner"*, C-140/20.

Cass. pen., Sez. VI, 14 aprile 2023, n. 15836.

Corte giust. UE, 30 aprile 2024, C-178/22.