https://doi.org/10.60923/issn.1825-1927/22568 ISSN 1825-1927

La riforma della *data retention* a fini di contrasto della criminalità

Tra evoluzione tecnologica e garanzia dei diritti

Mario Luberto [1]

[1] Università degli Studi di Modena e Reggio Emilia, Dipartimento di Giurisprudenza

Abstract: Con il D. L. n. 132 del 30.09.2021, convertito con modificazioni dalla L. n. 178 del 23.11.2021, il legislatore italiano ha profondamente modificato l'art. 132 D.lgs. n.196 del 30.06.2003, ovvero la disposizione dedicata alla conservazione ed all'acquisizione dei dati di traffico telefonico e telematico a fini di prevenzione e contrasto della criminalità (c.d. *data retention*). Come risulta anche dal testo del decreto legge, la riforma è stata generata dalla pronuncia della Grande sezione della Corte di Giustizia UE del 2.3.2021 (causa C-746/18, *H.K.* contro *Prokuratuur*). Il contributo, dopo aver delineato i tratti dell'istituto in questione ed aver ripercorso i principali arresti della Corte di Giustizia in materia di *data retention*, si propone di mettere in luce come le modifiche legislative apportate non soltanto appaiano in linea con l'evoluzione delle tecnologie utilizzate a fini di sorveglianza digitale, ma rappresentino altresì un significativo passo in avanti nella garanzia dei diritti fondamentali. L'articolo si sofferma infine su alcune criticità della disciplina, non risolte dall'intervento riformatore qui commentato.

Keywords: Sorveglianza digitale, Data retention, Criminalità, Mezzi di ricerca della prova, Diritti fondamentali.

1 Introduzione

E' stato osservato come l'ordinamento giuridico dell'Unione Europea si sia sviluppato in gran parte come un diritto giurisprudenziale, affidato alla funzione nomofilattica della Corte di giustizia[1]. In questo processo di sviluppo, principi di pari importanza enunciati nei trattati sarebbero stati perseguiti e raggiunti in modo oggettivamente disomogeneo ed il mercato interno avrebbe privilegiato la stabilità dei prezzi rispetto alle politiche miranti alla piena occupazione, al progresso sociale e alla lotta all'esclusione e alle discriminazioni sociali[2]. Ciò nonostante, appare significativo il percorso tracciato dalla Corte di Giustizia dell'Unione Europea (CGUE) a favore di diritti sanciti dalla Carta dei Diritti Fondamentali dell'Unione Europea (CDFUE) -oltre che da altre fonti, comunitarie e non- quali il diritto alla riservatezza (art. 7 CDFUE) ed il diritto alla protezione dei dati personali (art. 8 CDFUE). E' noto che, mentre il diritto alla riservatezza consiste nella libertà di non subire

mluberto@unimore.it (Mario Luberto);

1. Omaggio V., *I diritti oltre lo Stato. La governance europea e la crisi dei diritti*, in *Rivista di Filosofia del Diritto*, 1, 2021, p.38. Il modello di tutela dei diritti costruito in via giurisprudenziale dalla Corte di giustizia, soprattutto prima dell'adozione della Carta dei diritti fondamentali dell'UE, appare connotato dal fatto di rimettere all'attività del giudice l'individuazione delle fattispecie tutelabili e la misura della tutela. Caretti P.- Tarli Barbieri G. *I Diritti Fondamentali. Libertà e Diritti sociali*, Giappichelli, 2022, pp. XXXI-XXXII

2. Ibidem, p.39.

interferenze nella propria vita privata, il diritto alla protezione dei dati personali si manifesta nel controllo del trattamento e della circolazione dei dati che riguardano la propria persona[3], la cosiddetta autodeterminazione informativa. Come annotato[4], il giudice europeo si è sinora dimostrato, rispetto alle giurisprudenze nazionali, di maggiore sensibilità sui temi -di impronta tipicamente eurounitaria- del diritto alla privacy e del trattamento dei dati personali. D'altra parte, il sempre più diffuso utilizzo di Internet comporta che proprio sul Web la vita privata sia maggiormente esposta a rischi di violazione e che le conseguenti misure di protezione debbano essere perciò adottate, a pena della loro inefficacia, a livello sovranazionale[5]. La rete può "sfuggire" alle norme statuali.

Circa l'attenzione della Corte europea per il diritto alla riservatezza ed il diritto alla privacy, ci si può soffermare innanzi tutto su alcune storiche decisioni, note come sentenze "*Google Spain"*,"*Schrems 1*" e "*Schrems 2*".

Con la prima, celebre pronuncia[6], resa il 13.5.2014 (causa C-131/12, *Google Spain SL.* e *Google Inc.* contro *AEPD* e *González*) la Grande Sezione ha affrontato il tema del "diritto all'oblio" in rete[7] ed ha configurato (§§ 88 e 99) a carico del gestore di un motore di ricerca l'obbligo di "deindicizzazione", ovvero l'obbligo di sopprimere, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, i link verso pagine web pubblicate da terzi e contenenti informazioni alla stessa persona relative. Ciò anche nei casi in cui tale nome o tali informazioni non vengano cancellati dalle suddette pagine web o la loro pubblicazione sia di per sé lecita. L'obbligo di deindicizzazione verrebbe meno, secondo la Corte, solo se per ragioni particolari l'ingerenza nei diritti alla riservatezza ed alla protezione dei dati di natura personale risultasse giustificata dall'interesse prevalente del pubblico ad avere accesso all'informazione[8].

Altri due arresti della Grande Sezione della Corte di giustizia ci introducono al tema della sorveglianza "digitale" – ovvero effettuata con il supporto di tecnologie digitali[9]- da parte di autorità pubbliche. Le sentenze in questione sono la sentenza del 6.10.2015 (causa C-362/14, *Maximilian Schrems* contro *Data Protection Commissioner*, nota come *Schrems 1)* e la sentenza del 16.7.2020 (causa C-311/18, *Data Protection Commissioner* contro *Facebook Ireland Ltd* e *Maximilian Schrems*, la cosiddetta *Schrems 2)*[10]. Come noto, a differenza di quanto avviene nell'Unione Europea, negli Stati Uniti la tutela dei dati personali è fornita attraverso un quadro normativo frammentato, costituto da un sistema di leggi statali e federali e da numerosi precedenti giurisprudenziali[11]. In entrambe le cause, la Corte di Lussemburgo ha dichiarato invalide le decisioni con le quali la Commissione europea aveva considerato adeguati alla protezione dei dati personali gli accordi Ue-USA, concernenti il trasferimento di tali dati dall'Unione Europea agli Stati Uniti. Nelle fattispecie *de quibus* si trattava di dati personali trasferiti da parte di Facebook Ireland Ltd verso la propria società controllante Facebook Inc. situata negli *States*. Dati che potevano poi essere sottoposti ad accesso ed utilizzati dalle autorità pubbliche di *intelligence* statunitensi, sulla base di programmi di sorveglianza per fini di sicurezza nazionale.

Con la sentenza *Schrems 1* la Corte ha dichiarato invalida la decisione 2000/520/CE del 26.7.2000, con cui la Commissione europea aveva constatato che gli Stati Uniti d'America, mediante i principi dell'accordo *Safe*

3. Tra molti, Terolli E., *Privacy e protezione dei dati personali Ue vs. Usa. Evoluzioni di diritto comparato e il trasferimento dei dati dopo la sentenza "Schrems II"*, in *Il diritto dell'informazione e dell'informatica*, 1, 2021, p.51.

4. Torre F., *Data retention: una ventata di "ragionevolezza" da Lussemburgo (a margine della sentenza della Corte di giustizia 2 marzo 2021, c-746/18)*, in *Consulta online*, III , p.546.

5. Sambuco G., *Note in tema di data retention*, in *Archivio penale Web*, 2, 2022, pp.3-4.

6. In *https://curia.europa.eu*.

7. Ad oggi disciplinato dall'art. 17 del Regolamento Ue 2016/679.

8. Con la sentenza del 24.09.2019 (C-507/17, in *https://curia.europa.eu*) la Corte di giustizia ha precisato che il gestore del motore di ricerca non è tenuto ad effettuare la deindicizzazione in tutte le versioni del motore di ricerca, ma solo nelle versioni del motore corrispondenti a tutti gli Stati membri dell'Unione Europea.

9. Orrù E., *Verso un nuovo panottico? La sorveglianza digitale.*, in Casadei T.-Pietropaoli S. (a cura di), *Diritto e tecnologie informatiche*, seconda edizione ampliata ed aggiornata, Wolters Kluwer, 2024, p. 232.

10. Entrambe reperibili su *https://curia.europa.eu*.

11. Terolli E., cit, p. 77.

Harbour, assicuravano un livello di protezione adeguato ai dati personali provenienti dall'Unione Europea verso organizzazioni aventi sede negli USA. La Corte ha rilevato, tra l'altro, che i principi dell'accordo erano applicabili soltanto alle organizzazioni americane autocertificate e non alle autorità pubbliche americane (§ 82); che la decisione non conteneva alcuna dichiarazione quanto all'esistenza, negli Stati Uniti, di norme destinate a limitare le eventuali ingerenze da parte delle autorità statali -sebbene autorizzate dal perseguimento di fini legittimi, come la sicurezza nazionale- nei diritti fondamentali delle persone i cui dati fossero trasferiti verso gli USA (§ 88); che la decisione medesima non menzionava l'esistenza di una tutela giuridica efficace nei confronti delle ingerenze di tale natura. Secondo la Corte, in particolare, i meccanismi di arbitrato privato e i procedimenti dinnanzi alla Commissione federale per il commercio, di cui al *Safe Harbour*, non potevano essere applicati alle controversie concernenti le ingerenze nei diritti fondamentali risultanti da misure di origine statale (§ 89).

La successiva sentenza *Schrems 2*, ha invalidato anche la decisione di adeguatezza dell'accordo UE-USA denominato *Privacy Shield*, che aveva sostituito il precedente *Safe Harbour*. Secondo il giudice europeo le attività di intelligence delle autorità statunitensi venivano, nel predetto accordo, ammesse in termini che violavano la Carta dei diritti fondamentali UE. I programmi di sorveglianza statunitensi -che comportavano un'ingerenza nei diritti al rispetto della vita privata e familiare ed alla protezione dei dati personali- non risultavano rispettosi né dei criteri, sanciti dall'art. 52, par.1, CDFUE[12], che debbono presiedere alla limitazione dei diritti e delle libertà riconosciuti dalla Carta (§ 184 della sentenza), né del diritto ad una tutela giurisdizionale effettiva di cui all'art. 47 CDFUE (§ 192). Quanto ai criteri dell'art. 52, la normativa statunitense non prevedeva l'esistenza di limitazioni all'attuazione dei programmi di sorveglianza, né diritti azionabili dagli interessati nei confronti delle autorità statunitensi davanti ai giudici. Così risultando violato il diritto dell'Unione sotto il profilo del principio di proporzionalità, dal momento che i predetti programmi di sorveglianza non potevano considerarsi limitati allo stretto necessario (§§ 180-184). Quanto al diritto alla tutela giurisdizionale, la figura del Mediatore, prevista nel *Privacy Shield* -quale meccanismo di vigilanza sull'accesso e sull'utilizzo dei dati personali per motivi di sicurezza nazionale- non è apparsa alla Corte conforme all'art. 47, comma secondo, CDFUE, per il quale ogni individuo ha diritto a che la sua causa sia esaminata da un giudice indipendente e imparziale. Si era infatti dinanzi ad una figura, parte integrante del Dipartimento di Stato degli Stati Uniti, della quale non risultavano fornite adeguate garanzie di indipendenza rispetto al potere esecutivo (§ 195). Inoltre, la decisione della Commissione europea non conteneva alcuna indicazione circa l'autorizzazione del Mediatore ad adottare decisioni vincolanti nei confronti dei servizi statunitensi di intelligence (§ 196). La situazione di incertezza seguita alle sentenze *Schrems* è stata risolta il 10.7.2023, con la decisione di adeguatezza della Commissione del nuovo accordo *Data privacy Framework* sul trasferimento di dati personali tra Unione Europea e Stati Uniti.

2 La sentenza *H.K.* contro *Prokuratuur*

Nel marzo 2021 la Corte di Giustizia si è pronunciata specificatamente (e nuovamente) sull'istituto della c.d. *data retention*. L'espressione designa l'obbligo, da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazioni, di conservare per un determinato periodo di tempo i dati del traffico telefonico e telematico a fini di prevenzione, accertamento e perseguimento di reati. Dati di cui i fornitori dei servizi sono in possesso per ragioni commerciali o esigenze di fatturazione. La *retention* non concerne il contenuto della comunicazione, bensì i "metadati", ovvero i dati esterni alla comunicazione medesima. Vi rientrano il numero del chiamante o del chiamato, la data, l'ora e la durata della comunicazione, il *device* utilizzato, le celle telefoniche "agganciate" dall'apparecchio e perciò la sua ubicazione, il tipo di connessione, l'indirizzo IP, i dati di identificazione dell'abbonato o dell'utente registrato. Le informazioni

12. L'art. 52 (*Portata e interpretazione dei diritti e dei principi*), paragrafo 1, dispone che "Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui".

ricavate riguardano anche sms, mms, email, siti visitati[13]. Tra i dati esterni acquisibili si ritiene debbano essere inclusi anche quelli relativi alle chiamate effettuate a mezzo dei sistemi *VOIP* (*Voice over IP*)[14]. Tutti questi metadati acquisiti *post factum* sono detti anche tabulati, alludendo al supporto documentale su cui vengono poi incorporati[15]. Peraltro, i tabulati possono rappresentare uno strumento di localizzazione utilizzabile non solo *ex post*, ma anche in tempo reale, mediante la già menzionata rilevazione delle celle di aggancio dei telefoni[16]. Trattasi della tecnica del tracciamento telefonico (c.d. positioning), alla quale si può affiancare, quale ulteriore strumento di "pedinamento elettronico", la localizzazione satellitare a mezzo GPS. Va invero precisato che sulla riconduzione del c.d *positioning* e della localizzazione a mezzo GPS alla normativa concernente la conservazione e l'acquisizione dei dati di traffico telefonico e telematico non vi è uniformità di vedute[17]. E' altresì dibattuto se i *file di log* siano sottoposti alle medesime tutele previste dall'istituto della *data retention*[18]. Sulla distinzione tra dati esterni e contenuto della comunicazione invece si tornerà.

La sentenza in questione, nota anche come sentenza H.K., è stata resa dalla Grande sezione della Corte di Giustizia il 2.3.2021 (causa C-746/18, *H.K.* contro *Prokuratuur*)[19]. La pronuncia ha avuto dirette conseguenze

13. Murro O., *Dubbi di legittimità costituzionale e problemi di inquadramento sistematico della nuova disciplina dei tabulati,* in *Cassazione penale*, 6, p.2442.

14. Baccari G.M., *Il trattamento (anche elettronico) di dati personali per finalità di accertamento di reati*, in Cadoppi A.-Canestrari S.-Manna A.- Papa M. (diretto da), *Cybercrime*, seconda edizione, Utet Giuridica, 2023, p.1876.

15. Marcolini S., *L'istituto della data retention tra legalità interna ed internazionale*, in Cadoppi A.-Canestrari S.-Manna A.- Papa M. (diretto da) *Cybercrime*, Utet Giuridica, 2019, p.1581.

16. Murro O., 2022, cit., p.2442.

17. Alcuni autori sostengono che sia la localizzazione satellitare tramite GPS, sia il tracciamento telefonico (c.d. *positioning*) richiedano la procedura prevista per l'acquisizione dei dati di traffico telefonico e telematico a fini penali dall' art.132 D.lgs. n.196 del 30.6.2003. In tal senso, si vedano: Filippi L., *Tabulati telefonici e telematici e rispetto della vita privata*, in *Diritto di difesa,* 2022, pp. 5-6*;* Spangher G., *I tabulati: il regime transitorio…in attesa degli effetti generati dallo tsunami della nuova sentenza della Corte di giustizia*, in *Giustizia insieme*, 27.4.2022. Diversa l'opinione (Pestelli G., *Convertito in legge il D.L. 132/2021: le modifiche apportate (e quelle mancate) in materia di tabulati*, in *Altalex* , 18.11.2022) di chi ha rilevato come nell'attuale art.132 D.lgs. n.196 del 30.6.2003, riguardante la *data retention,* il legislatore nulla abbia previsto in merito al pedinamento mediante GPS e al *positioning* e come ciò induca a ritenere che tali fattispecie esulino dal contenuto applicativo della norma. Secondo altri (Demartis F., *La nuova disciplina sui tabulati: un completo adeguamento agli standard europei?*, in *Diritto penale e processo*, 3, 2022, p.307), occorre distinguere tra i casi in cui i dati di ubicazione siano detenuti dal gestore a prescindere dall'esistenza di traffico telefonico o telematico ed i casi nei quali invece i dati di ubicazione sono detenuti dal gestore in ragione del traffico telefonico e telematico. Solo in tale ultima ipotesi si tratterebbe di dati ricompresi nei tabulati di cui all'art. art.132 D.lgs. n.196 del 30.6.2003. La mancanza di un'espressa disciplina per l'attività di acquisizione dei dati di ubicazione quando non sono in corso attività di comunicazione potrebbe fondare una questione di legittimità costituzionale per violazione del principio di ragionevolezza, oppure condurre alla diretta applicazione della normativa sovranazionale (Murro O., *La geolocalizzazione tramite celle telefoniche. Soluzioni percorribili, in un mondo digitale in trasformazione*, in *Diritto penale e processo,* 8, 2023, pp.1089-1090). Peraltro, in un caso di comunicazioni tra correi mediante telefoni cellulari, la Corte di Cassazione (Sezione quinta penale, sentenza n. 8968 del 24.2.2022, in *www.cortedicassazione.it*) ha ritenuto che la nozione di dati relativi al traffico comprenda anche quelli che indicano il luogo della comunicazione, mentre i dati relativi all'ubicazione sarebbero unicamente quelli che afferiscono alla localizzazione di un'apparecchiatura. Pertanto, secondo la Corte, le "celle" agganciate da una comunicazione telefonica rientrano -in quanto "dati relativi al traffico telefonico"- nella disciplina dei tabulati. Anche la successiva sentenza della Corte di Cassazione (Sez. VI penale, n. 15836 del 14.4.2023, in *Processo Penale e Giustizia*), ha argomentato che, una volta che una persona abbia prescelto l'uso del mezzo telefonico, in forza dell'art.15 della Costituzione vada riconosciuto il diritto di mantenere segreti tanto i dati che possano portare all'identificazione dei soggetti della conversazione, quanto quelli relativi al tempo e al luogo dell'intercorsa comunicazione. Una recente decisione della Suprema Corte (Sezione seconda penale, sentenza n. 27513 del 2.7.2025, in *https://www.cortedicassazione.it*) si è inoltre espressa sulla legittimità dell'uso a fini probatori dei dati di *positioning* emersi dal rilevamento del sistema GPS installato su un'autovettura. Nella specie, la Corte ha statuito che il c.d. pedinamento elettronico tramite il sistema satellitare GPS non implica un accumulo di dati sensibili da parte del gestore del servizio, che le relative risultanze non rientrano nella disciplina della data retention e che esse sono, pertanto, utilizzabili senza necessità di autorizzazione preventiva da parte dell'Autorità Giudiziaria. Dello stesso tenore anche la sentenza della Corte di Cassazione, sezione seconda penale, n. 19038 del 9.05.2025 (In banca dati *Dejure*), secondo la quale la localizzazione degli spostamenti tramite sistema di rilevamento satellitare GPS è mezzo di ricerca della prova atipico, le cui risultanze sono utilizzabili senza necessità di autorizzazione da parte dell'autorità giudiziaria, non trovando applicazione per analogia né la disciplina di cui all'art. 132, comma 3, D.Lgs. 30 giugno 2003, n. 196, in tema di tabulati, né i principi affermati dalla giurisprudenza della Corte di Giustizia dell'Unione Europea in materia di data retention.

18. Si veda in merito: Della Torre J.-Malacarne A., *L'utilizzo dei file di log per scopi di contrasto alla criminalità: nodi problematici e possibili soluzioni*, in *Archivio penale Web*, 2, 2022, pp. 1-22. Circa la riconducibilità dei *file di log* alla normativa concernente la *data retention* si segnala un'ordinanza del 26.6.2025, di rinvio pregiudiziale alla Corte di Giustizia europea, del Giudice per le indagini preliminari presso il Tribunale di Catania, meglio descritta alla nota 174 del presente elaborato.

19. In *Giurisprudenza penale web*.

nell'ordinamento giuridico italiano in quanto, per adeguarsi ad essa, pochi mesi dopo il nostro legislatore ha riformato l'articolo 132 del D.lgs. n.196 del 30.06.2003 (di qui innanzi anche Codice della Privacy o Cod. Priv.), ovvero la disposizione che delinea presupposti e procedura della conservazione e dell'acquisizione dei dati esterni delle comunicazioni per finalità di accertamento e repressione di reati. Disposizione che è stata in questi anni oggetto di numerosi interventi legislativi[20]- la relativa disciplina, si è detto, sembra vivere una "perenne emergenza"[21]- volti a contemperare le esigenze di protezione della riservatezza con quelle connesse alla sicurezza pubblica. Si tratta, evidentemente, di una norma "strategica", la cui rilevanza varca i confini della protezione dei dati personali per coinvolgere anche altri diritti fondamentali, nonché la tematica dei mezzi di ricerca della prova in genere. Tanto è vero, che si è ritenuto che sarebbe stato preferibile, in sede della sopra citata riforma, collocare la disciplina dei tabulati nel Codice di procedura penale, dopo le disposizioni sulle intercettazioni[22].

Nella fattispecie, riguardante l'ordinamento dell'Estonia, l'imputata era stata condannata (per reati di furto, utilizzo della carta bancaria di un terzo e di violenza verso persone partecipanti ad un procedimento giudiziario) grazie all'acquisizione sia di dati relativi a vari numeri di telefono, sia di codici internazionali di identificazione di apparecchiatura di telefonia mobile. I dati erano stati raccolti dall'autorità incaricata delle indagini su autorizzazione della Procura distrettuale.

La Corte, a seguito di ricorso pregiudiziale ai sensi dell'art. 267 del Trattato sul Funzionamento dell'Unione Europea, ha sancito diversi principi.

In primo luogo, ha affermato che " *(…) l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, deve essere interpretato nel senso che esso osta ad una normativa nazionale, la quale consenta l'accesso di autorità pubbliche ad un insieme di dati relativi al traffico o di dati relativi all'ubicazione, idonei a fornire informazioni sulle comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica o sull'ubicazione delle apparecchiature terminali da costui utilizzate e a permettere di trarre precise conclusioni sulla sua vita privata, per finalità di prevenzione, ricerca, accertamento e perseguimento di reati,* ***senza che tale accesso sia circoscritto a procedure aventi per scopo la lotta contro le forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza pubblica*** *(enfasi aggiunta, n.d.a)*, e ciò indipendentemente dalla durata del periodo per il quale l'accesso ai dati suddetti viene richiesto, nonché dalla quantità o dalla natura dei dati disponibili per tale periodo"* (§ 45). Dunque, solo a fronte di *"forme gravi di criminalità"* o di *"gravi minacce alla sicurezza pubblica"* una normativa nazionale può autorizzare le autorità pubbliche ad ingerenze che consentano "*di trarre precise conclusioni sulla vita privata"*. Questo tipo di ingerenza nei diritti di cui articoli 7 e 8 della CDFUE presenta infatti in ogni caso un carattere grave (§ 39). Tale principio della sentenza H.K. ha rappresentato un primo profilo di criticità dell'art. 132 del Codice della privacy che, per come formulato al momento della pronuncia, non specificava i reati per i quali si potesse procedere alla conservazione ed all'acquisizione dei dati di traffico. La disposizione al tempo si limitava (al comma 5-bis, tuttora vigente) a prevedere un periodo più lungo di conservazione dei dati per i delitti commessi con finalità di terrorismo e per quelli per i quali l'art. 407, comma 2, lettera a) del codice di rito contempla un termine massimo di durata delle indagini preliminari di due anni.

Pertanto, la Corte di giustizia ha innanzi tutto circoscritto il ricorso alla *data retention* mediante il criterio consistente nello scopo del contrasto a forme gravi di criminalità o della prevenzione di gravi minacce alla sicurezza pubblica. Nel paragrafo 50 la sentenza H.K ha posto argini anche da un punto di vista dei soggetti

20. Basti ricordare che l'art.132 era già stata modificato dal D.L. n. 354 del 24,12 2003, convertito con modificazioni dalla legge di conversione 26.2.2004; successivamente dal D.L. 27.7.2005, n. 144, convertito, con modificazioni, dalla legge di conversione n. 45 del 31.7.2005, n. 155, recante misure urgenti per il contrasto del terrorismo internazionale; dalla l. n. 48 del 18.3.2008, di ratifica ed esecuzione della Convenzione del Consiglio d´Europa sulla criminalità informatica fatta a Budapest il 23.11.2001; dal D.lgs. n.109 del 30.5.2008, di attuazione della direttiva 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 direttiva 2002/58/CE. Per una più approfondita disamina di tutte le modifiche intervenute prima della recente riforma dell'art. art.132 D.lgs. n.196 del 30.6.2003 si veda Baccari G. M., cit., pp.1871-1881.

21. Todaro G., *L'evoluzione delle fonti del diritto nella "società algoritmica": data retention e diritti fondamentali della persona*, in *Cassazione Penale*, 6, 2024, p. 2016.

22. Filippi L., *Tabulati telefonici e telematici e rispetto della vita privata*, 2022, cit., p.13.

destinatari dell'accesso ai dati personali. Secondo il tenore del paragrafo, l'accesso ai dati conservati può essere consentito, al fine della lotta contro la criminalità, soltanto per i dati di persone sospettate di progettare, di commettere o di aver commesso un illecito grave, o di esservi implicate. Solo in situazioni particolari, come quelle in cui interessi vitali della sicurezza nazionale, della difesa o della sicurezza pubblica siano minacciati da attività di terrorismo, l'accesso ai dati di altre persone (ad es. testimoni) potrebbe essere concesso. In tal caso, occorre tuttavia che vi siano elementi oggettivi che permettano di ritenere che tali dati potrebbero, in un caso concreto, fornire un contributo effettivo alla lotta contro le suddette attività criminali. Anche questo limite risulta non rispettato dall'art. 132 del Codice della privacy il quale, nonostante la riforma, non reca a tutt'oggi alcun riferimento alle persone i cui dati possono essere oggetto di accesso.

Altra importante statuizione della Corte concerne l'autorità che può autorizzare l'accesso ai dati conservati. Ad avviso della CGUE questa autorità non può essere il Pubblico Ministero. Secondo quanto recita la sentenza (§59) "(…) *l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, 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"*. Da una parte infatti, è essenziale che l'accesso sia subordinato ad un controllo preventivo effettuato o da un giudice o da un'entità amministrativa indipendente e che la decisione di tale giudice o di tale entità intervenga a seguito di una richiesta motivata (§ 51). Salvi casi di urgenza, debitamente giustificati, nei quali il controllo deve comunque avvenire in termini brevi (§ 58). Dall'altra, il requisito di indipendenza dell'autorità incaricata di esercitare il controllo preventivo impone che tale autorità abbia la qualità di terzo rispetto a quella che chiede l'accesso ai dati. In ambito penale, il requisito di indipendenza implica che l'autorità incaricata di tale controllo preventivo non sia coinvolta nella conduzione dell'indagine penale e abbia una posizione di neutralità nei confronti delle parti del procedimento penale (§ 54). Ciò non si verifica nel caso di un pubblico ministero che dirige il procedimento di indagine ed esercita, se del caso, l'azione penale (§ 55). Né è sufficiente a conferire al Pubblico Ministero la qualità di terzo la circostanza che tale organo sia tenuto a verificare gli elementi a carico e quelli a discarico, a garantire la legittimità del procedimento istruttorio e ad agire unicamente in base alla legge ed al suo convincimento (§ 56).

Anche in considerazione del requisito di indipendenza, così come interpretato dalla Corte, l'art. 132 D.lgs. n.196 del 30.06.2003 non appariva compatibile con la normativa europea, atteso che il comma 3 disponeva che i dati fossero acquisiti con decreto del Pubblico Ministero.

Consapevole di queste criticità, il legislatore ha novellato il predetto art. 132[23] mediante l'art. 1 del D.L. n.132 del 30.09.2021 -convertito con modificazioni dalla L. n. 178 del 23.11.2021- che ha sostituito il comma 3 ed introdotto tre nuovi commi, il 3-bis, il 3-ter ed il 3-quater. In sintesi, la novella ha individuato tassativamente i reati per i quali è possibile procedere all'acquisizione dei dati di traffico[24]; ha specificato ulteriori presupposti per la legittimità dell'acquisizione (i "sufficienti indizi di reati" e la loro "rilevanza" per l'accertamento dei fatti); ha previsto la giurisdizionalizzazione della procedura (è richiesta una previa autorizzazione del giudice oppure, nei casi in cui i dati siano già stati acquisiti per ragioni di urgenza, una sua successiva autorizzazione entro termini stringenti); ha comminato la sanzione dell'inutilizzabilità dei dati acquisiti in caso di violazione della procedura. Con la legge di conversione è stata inoltre introdotta una disciplina transitoria che consente l'applicazione "retroattiva" della nuova procedura[25].

23. E' lo stesso D.L. n.132 del 30.09.2021 a ritenere *" (..) la straordinaria necessità ed urgenza di garantire la possibilità di acquisire dati relativi al traffico telefonico e telematico per fini di indagine penale nel rispetto dei principi enunciati dalla Grande sezione della Corte di giustizia dell'Unione europea nella sentenza del 2 marzo 2021, causa C-746/18 (…)*".

24. Ai sensi dell'art. 132, comma 3, n.196 del 30.06.2003 deve trattarsi di delitti per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, determinata a norma dell'articolo 4 del codice di procedura penale, 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.

25. Art.1, comma 1-bis, L. 23.11. 2021 n.178 : "I dati relativi al traffico telefonico, al traffico telematico e alle chiamate senza risposta, acquisiti nei procedimenti penali in data precedente alla data di entrata in vigore del presente decreto, possono essere utilizzati a carico dell'imputato solo unitamente ad altri elementi di prova ed esclusivamente per l'accertamento dei reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, determinata a norma dell'articolo 4 del codice di procedura penale, e dei reati di minaccia e di molestia o disturbo alle persone con il mezzo del telefono, quando la minaccia, la

3 I precedenti (e non solo) della Corte di Giustizia sulla *data retention*

I principi enunciati nella sentenza in commento si inseriscono in un consolidato filone interpretativo della Corte di Giustizia, inaugurato da due ben note sentenze della Grande Sezione: la sentenza *Digital Rights Ireland* dell'8.4.2014[26] (causa C-293/12, *Digital Rights Ireland Ltd contro Minister for Communications, Marine and Natural Resources ed altri*) e la sentenza *Tele2 Sverige* del 21.12.2016[27] (cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB contro Post-och telestyrelsen*; *Watson ed altri contro Secretary of State for the Home Department*).

Con la sentenza *Digital Rights Ireland* la CGUE ha dichiarato invalida la Direttiva 2006/24/CE del Parlamento europeo e del Consiglio del 15.3.2006 (c.d. Direttiva Frattini) -di modifica della Direttiva 2002/58/CE (Direttiva *E-privacy*) - che riguardava la conservazione dei dati personali generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione. La Direttiva violava infatti, a giudizio della Corte, i limiti imposti dal rispetto del principio di proporzionalità alla luce della Carta dei Diritti Fondamentali dell'UE (§ 69). Nella pronuncia si possono reperire enunciazioni poi riprese dalla sentenza H.K.: al § 60 è dato leggere che la Direttiva n. 2006/24/CE non prevedeva alcun criterio oggettivo che consentisse di circoscrivere ai reati che possano essere considerati sufficientemente gravi sia l'accesso delle autorità nazionali competenti ai dati, sia l'uso dei medesimi a fini di prevenzione, di accertamento o di indagini penali; al § 58 è stato rilevato invece come la Direttiva riguardasse in maniera globale l'insieme delle persone che fanno uso dei mezzi di comunicazione elettronica, senza tuttavia che le persone i cui dati venissero conservati si dovessero trovare, anche indirettamente, in una situazione che potesse dare luogo ad indagini penali; al § 62 la Corte ha osservato come l'accesso ai dati conservati da parte delle autorità nazionali competenti non fosse subordinato ad un previo controllo effettuato da un giudice o da un'autorità amministrativa indipendente, la cui decisione fosse diretta a limitare l'accesso ai dati e il loro uso a quanto strettamente necessario per raggiungere l'obiettivo perseguito[28].

Invalidata la Direttiva n. 2006/24/CE, sino ad allora la fonte della disciplina europea della *data retention*, i parametri normativi di riferimento sono divenuti l'art. 15, paragrafo 1, della già menzionata Direttiva sulla protezione dei dati personali e della vita privata nell'ambito delle comunicazioni elettroniche (n. 2002/58/CE) e la Carta dei Diritti Fondamentali dell'Unione Europea (CDFUE). L'art. 15 paragrafo 1 della Direttiva n. 2002/58/CE reca gli obiettivi (la salvaguardia della sicurezza nazionale, della difesa, della sicurezza pubblica, nonché la prevenzione, la ricerca, l'accertamento ed il perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica) ed i principi (di legalità e proporzionalità) nel rispetto dei quali le legislazioni degli Stati membri possono legittimamente limitare i diritti e gli obblighi di cui alla direttiva medesima[29]. La disposizione deve essere interpretata in riferimento alla CDFUE ed in particolare al

molestia o il disturbo sono gravi".

26. In *https://curia.europa.eu*.

27. In https://eur-lex.europa.eu.

28. Le argomentazioni e le conclusioni della sentenza *Digital Rights Ireland* erano state sostanzialmente anticipate da due decisioni, una della Corte Costituzionale tedesca del 2010, l'altra della Corte Costituzionale romena del 2009, entrambe vertenti sulle legislazioni nazionali di attuazione della c.d. direttiva Frattini in materia di *data retention*. Nelle sentenze, le normative esaminate sono state giudicate incostituzionali per violazione dei principi di stretta necessità, di proporzionalità, nonché di certezza, determinatezza e trasparenza che devono presiedere alla limitazione dei diritti fondamentali. Si veda Flor R., *La tutela dei diritti fondamentali della persona nell'epoca di internet. Le sentenze del Bundesverfassungsgericht e della Curtea Constitutionalâ su investigazioni ad alto contenuto tecnologico e data retention*, in Picotti L.-Ruggieri F. (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica,* Giappichelli, 2011, in particolare pp. 45-46.

29. "Gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva [95/46], una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica, e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l'altro adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo. Tutte le misure di cui al presente paragrafo sono conformi ai principi generali del diritto dell'Unione, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea". Vi è chi ha messo in evidenza la vaghezza del dettato normativo e come il richiamo agli ampi requisiti di "necessità", "opportunità" e "proporzionalità all'interno di una società democratica" abbia determinato difformità interpretative tra gli Stati membri. Formici G., *La data retention saga*

già menzionato art. 52 paragrafo 1 (sulle eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla Carta), nonché agli artt. 7 ("Rispetto della vita privata e della vita familiare"), 8 ("Protezione dei dati di carattere personale") ed 11 ("Libertà di espressione e d'informazione"). Pertanto, ad oggi le questioni trattate dalla Corte europea sulla conservazione dei dati personali ai fini di prevenzione ed accertamento di reati vertono sulla conformità delle legislazioni nazionali, di volte in volta esaminate, all'articolo 15, paragrafo 1, della Direttiva 2002/58/CE, letto in riferimento agli articoli 7, 8 e 11, nonché all'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea.

Con la pronuncia *Tele2 Sverige* la Grande Sezione ha sostanzialmente ribadito le proprie precedenti statuizioni ed ha dichiarato che l'articolo 15, paragrafo 1, della direttiva 2002/58/CE, interpretato alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della CDFUE osta ad una normativa nazionale sulla *data retention* la quale, nell'ambito della lotta contro la criminalità, non limiti tale accesso alle sole finalità di lotta contro la criminalità grave, non sottoponga l'accesso ai dati ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente e non esiga che i dati di cui trattasi siano conservati nel territorio dell'Unione (§ 125). La sentenza ha altresì precisato che un accesso generale a tutti i dati conservati che sia indipendente da una qualche connessione, almeno indiretta, con la finalità perseguita, non può essere considerato limitato allo stretto necessario. In linea di principio, un accesso può essere consentito, in relazione all'obiettivo della lotta contro la criminalità, soltanto per i dati di persone sospettate di progettare, di commettere o di aver commesso una violazione grave, o anche di essere implicate in una maniera o in un'altra in una violazione siffatta (§ 119).

Quanto deciso nelle sentenze *Digital Right Ireland* e *Tele 2 Sverige* (definite uno "tsunami" comunitario[30]) è stato ribadito ed approfondito da successive pronunce della Corte in materia. Tra le più recenti[31] si pongono la decisione della Grande Sezione del 5.4.2022 *(*causa C-140/20, *G.D. contro Commissioner of An Garda Siochána* ed altri[32]*)* e gli arresti "gemelli" del 20.09.2022 (Grande Sezione, cause riunite C-339/20 e C-397/20, *VD e SR*[33]; Grande Sezione, cause riunite C-793/19 e C.794/19, *Bundesrepublik* contro *SpaceNet Ag e Telekom Deutschland GmbH*[34]). La sentenza *Commissioner of An Garda Siochána* del 5.4.2022 ha, in particolare, ritenuto incompatibile con il diritto dell'Unione una conservazione generalizzata e indifferenziata dei dati relativi al traffico ed all'ubicazione per finalità di prevenzione delle minacce gravi alla sicurezza pubblica e di repressione della criminalità grave. Una così ampia conservazione di dati è, secondo la pronuncia (§58), ammissibile solo se adottata per fini di salvaguardia della sicurezza nazionale, purché ricorra una minaccia grave, reale ed attuale o comunque prevedibile, ed il provvedimento che impone al fornitore del servizio di comunicazione elettronica la conservazione dei dati sia assoggettato ad un controllo giurisdizionale effettivo e sia emesso per un periodo di tempo temporalmente limitato allo stretto necessario, rinnovabile in caso di persistenza della minaccia. Le finalità di lotta alla criminalità grave o di prevenzione di minacce gravi alla sicurezza pubblica (da tenere distinte, pertanto, da quella della salvaguardia della sicurezza nazionale[35]) pos-

al capolinea? Le ultime pronunce della CGUE in materia di conservazione dei metadati per scopi securitari, tra conferme e nuove aperture, in *DPCE online*, 1, 2021, p.1361.

30. Marcolini S., cit., p.1586.

31. Per un commento alle tre le sentenze: Filippi L., *Riservatezza e data retention: una storia infinita*, in *Penale Diritto e procedura*, 2022; Mucciarelli F, *Conservazione di dati di traffico di comunicazioni elettroniche e market abuse: una rilevante decisione della Corte di Giustizia dell'Unione Europe*, in *Sistema penale,* 2022; Resta F., *La corte di giustizia europea torna ancora sulla data retention*, in *Giustizia insieme*, 2022; Sambuco G., cit., pp. 9-12.; 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 Web,* 3, 2022, pp. 27-43; Flor R.-Marcolini S., *Dalla data retention alle indagini ad alto contenuto tecnologico*, Giappichelli, 2022, pp.84-89; Spangher G., *Data retention: non basta un restyling ora serve una vera riforma organica*, in *Guida al Diritto*, 17, 2022, pp.12-14; Di Stefano, G., *La Corte di Giustizia conferma la regola del divieto, con eccezioni, di conservazione dei dati di traffico telefonico e telematico ai fini di lotta alla criminalità grave: la fine della prova a mezzo di tabulati?*, in *Cassazione penale*, 1, 2023, pp.354-367.

32. In *https://curia.europa.eu.*

33. In *https://curia.europa.eu*

34. In *https://www.giustiziainsieme.it.*

35. La Corte ha ricordato (§ 61) che la preservazione della sicurezza nazionale "(…) corrisponde all'interesse primario di tutelare le funzioni essenziali dello Stato e gli interessi fondamentali della società mediante la prevenzione e la repressione delle attività tali da destabilizzare gravemente le strutture costituzionali, politiche, economiche o sociali fondamentali di un paese, e in particolare

sono legittimare (§ 101), entro limiti tracciati di volta in volta dalla sentenza (come la presenza di un controllo giurisdizionale effettivo o la limitazione del periodo di conservazione), solo misure di minor invasività, ovvero: una conservazione dei dati di traffico e di ubicazione "mirata", cioè delimitata, sulla base di elementi oggettivi e non discriminatori, attraverso criteri personali o geografici; una conservazione generalizzata e indifferenziata degli indirizzi IP e dei dati relativi all'identità anagrafica degli utenti; la possibilità di rivolgere ai fornitori di servizi di comunicazione elettronica un'ingiunzione per la conservazione rapida dei dati (*quick freeze*) anche oltre i termini legali. In termini pressoché identici si è espressa la già citata sentenza, sempre del 20.9.2022, *Bundesrepublik* contro *SpaceNet Ag e Telekom Deutschland GmbH*, in cui vengono tenute infatti distinte, rispettivamente, le fattispecie di conservazione generalizzata e indiscriminata per fini di sicurezza nazionale, di conservazione mirata, di conservazione generalizzata ed indiscriminata degli indirizzi IP, di conservazione generalizzata ed indiscriminata dei dati di identità anagrafica, di conservazione rapida dei dati. Peraltro, in un recente arresto[36] la Grande camera della Corte di Giustizia ha ulteriormente precisato che uno Stato membro può, al fine di conseguire un obiettivo connesso alla lotta contro i reati in generale, imporre ai fornitori di servizi di comunicazione elettronica un obbligo di conservazione generalizzata e indifferenziata degli indirizzi IP, ma solo assicurandosi che le modalità di conservazione di detti dati siano tali da garantire che sia esclusa qualsiasi combinazione degli indirizzi IP con altri dati conservati che consenta di trarre conclusioni precise sulla vita privata delle persone i cui dati si riferiscono e perciò, detto altrimenti, di profilarle. La pronuncia ha anche formulato in proposito alcune specifiche, riguardanti la struttura stessa della conservazione, che dovrebbe essere organizzata in modo da garantire una separazione effettivamente stagna delle diverse categorie di dati conservati. Questo approccio della giurisprudenza recente del giudice europeo -basato sulla valutazione congiunta dei due parametri costituiti dallo scopo perseguito attraverso la limitazione dei diritti fondamentali e dal grado di ingerenza delle misure- rappresenta una significativa declinazione del principio di proporzionalità ed era già stato seguito dalla Corte di Giustizia nella sentenza della Grande Sezione del 6.10.2020 (cause riunite C-511/18, C-512/18 e C-520/18, *La Quadrature du Net* ed altri contro *Premier ministre* ed altri, §. 168). Ma le sue radici affondano nell'ancor precedente sentenza *Ministerio Fiscal* resa il 2.10.2018 (Corte di Giustizia, Grande Sezione, causa C-207/16[37]), secondo cui l'accesso delle autorità pubbliche ai dati che consentono di identificare i titolari di carte SIM attivate con un telefono cellulare rubato (come il cognome, il nome ed eventualmente l'indirizzo) non costituisce un'ingerenza grave nei diritti fondamentali di questi e dunque non è tale da dover essere limitato alla lotta alla criminalità grave (§ 63)[38]. In definitiva, alla luce di tutti i limiti posti e dei distinguo formulati dalla giurisprudenza della Corte di giustizia, dovrebbero considerarsi illegittime le legislazioni dei paesi membri che prevedano la creazione di una "banca dati" alla quale attingere in caso di utilità o necessità investigativa[39].

Si può dunque constatare come la pronuncia H.K. si collochi in evidente continuità con i precedenti (ma, come si è visto, anche con gli arresti successivi) in materia di *data retention* e con le sentenze *Schrems*, così che si

da minacciare direttamente la società, la popolazione o lo Stato in quanto tale, quali in particolare le attività di terrorismo" e che la criminalità anche particolarmente grave non può essere equiparata a una minaccia per la sicurezza nazionale (§ 64). Di conseguenza, il fatto che i dati relativi al traffico e i dati relativi all'ubicazione siano stati legittimamente conservati per salvaguardare la sicurezza nazionale non legittima la loro conservazione anche ai fini della lotta contro la criminalità grave (§ 64). Vi è dunque, secondo il ragionamento della Corte, una gerarchia tra gli obiettivi che, a norma dell'art. 15, par. 1, Dir. 2002/58/CE, possono giustificare la limitazione dei diritti alla riservatezza e alla protezione dei dati personali nelle comunicazioni elettroniche. L'ordine gerarchico degli obiettivi fissati dalla direttiva è stato affermato dalla Corte di giustizia UE anche nella sentenza della Prima Sezione del 7.9.2023, causa C-162/22 (in *Altalex)*.

36. Sentenza del 30.4.2024 (causa c-470/21, *La Quadrature du Net ed altri*.), § 83, in *https://eur-lex.europa.eu*. Al successivo § 93 della sentenza, la Corte ha aggiunto che il quadro normativo deve altresì prevedere un periodo di conservazione limitato allo stretto necessario e assicurare, mediante norme chiare e precise, che la conservazione dei dati di cui trattasi sia subordinata al rispetto delle relative condizioni sostanziali e procedurali e che gli interessati dispongano di garanzie effettive contro i rischi di abuso nonché contro qualsiasi accesso a tali dati e qualsiasi uso illecito degli stessi.

37. In *https://curia.europa.eu*.

38. Peraltro, nel dibattito innanzi alla CGUE ed in seno al Consiglio dell'UE sulla *data retention* è emersa anche la possibilità di una "terza via" tra la conservazione mirata e quella generalizzata. Si tratta della conservazione *limitata* (*restricted data retention*), fondata sulla limitazione della conservazione solo a specifiche categorie di dati, nonché a determinati tipi di fornitori e di servizi. Formici, cit., p.1367.

39. Di Stefano G., cit., p. 363.

è parlato di una saga culminata nella sentenza H.K.[40], di una sentenza con cui la Grande Camera ha ribadito principi già perentoriamente affermati in passato[41], di un *fil rouge* che pare legare tutta la giurisprudenza della Corte[42], di un'impostazione non inedita[43].

Anche a proposito del principio, di cui alla medesima decisione H.K., secondo il quale l'acquisizione dei dati non può essere autorizzata dal Pubblico Ministero, non è ravvisabile a nostro avviso alcun repentino ed imprevedibile mutamento giurisprudenziale. Infatti, detto principio rappresenta un coerente sviluppo ed una specificazione di quello (da tempo sancito dalla Corte) per cui l'accesso ai dati conservati da parte delle autorità nazionali competenti deve essere subordinato ad un previo controllo effettuato da un giudice o da un'autorità amministrativa indipendente. In questo senso, la pronuncia si è limitata a chiarire in maniera inequivocabile il significato da attribuire alla nozione di "giudice", cui già la sentenza *Digital Right Ireland* alludeva[44]. Tanto è vero, che nella sentenza C-746 del 2.3.2021 qui in commento la necessaria terzietà dell'organo che autorizza l'accesso è argomentata nei §§ 54, 55 e 56 che trattano dell'indipendenza dell'organo che deve effettuare il controllo preventivo.

Per concludere sul punto, riteniamo che non sarebbe appropriato sostenere che la recente riforma dell'art. 132 Cod. Priv. sia stata generata da un *overruling* della Corte. Al contrario, trattasi di una riforma tardiva, i cui presupposti erano stati fissati dalla giurisprudenza eurounitaria sin dal 2014. Probabilmente, sono stati i vincoli derivanti dal Piano Nazionale di Ripresa e Resilienza (PNRR) a rendere non ulteriormente procrastinabile l'adeguamento del nostro ordinamento giuridico ai *dicta* della Corte di Giustizia[45].

4 Una riforma tra evoluzione tecnologica…

E' consolidata nella nostra giurisprudenza di legittimità la distinzione tra l'apprensione del contenuto di una conversazione, coperta dalle più garantiste disposizioni sulle intercettazioni di conversazioni o comunicazioni (artt. 266-271 c.p.p.), e l'acquisizione dei dati esterni alla comunicazione la quale, ritenuta di minor invasività, non necessiterebbe degli stessi presidi. La ragione della distinzione, ad oggi seguita anche dal legislatore (che affida la conservazione e l'acquisizione dei "tabulati" all'art. 132 Cod. Priv.), può essere ricostruita attraverso un pur sintetico richiamo alle decisioni rese dalle Sezioni Unite della Corte di Cassazione. La sentenza *Gallieri* [46] aveva invero asserito che il divieto di utilizzazione previsto dalla disciplina delle intercettazioni fosse riferibile, in caso di acquisizione avvenuta senza il prescritto decreto motivato dell'Autorità giudiziaria, anche all'acquisizione dei tabulati, ma è stata superata da altre due successive decisioni. Infatti, la sentenza *D'Amuri*[47], premessa la partizione tra dati interni (contenuto) e dati esterni (documentazione dei flussi di comunicazione avvenuti), ha considerato che "*la stampa e l'acquisizione dei dati esterni incidono sul loro "trattamento", costituendo una forma di intrusione nella sfera della riservatezza, diversa e minore rispetto all'intercettazione dei contenuti o dei dialoghi in corso"* e che intercettazioni ed acquisizione dei tabulati sono categorie disomogenee. Nello stesso senso anche la sentenza *Tammaro* [48] che ha condiviso l'approccio ermeneutico secondo cui non vi è omogeneità concettuale tra intercettazione di conversazioni e comunicazioni telefoniche, da una parte, ed acquisizione di tabulati dall'altra. L'impostazione può considerarsi seguita dalla sentenza Corte Costituzionale del 26.2.1993 n. 81[49]. La Consulta, pur riconoscendo che anche i

40. Greco C., *Quest'acquisizione non s'ha da fare: ennesimo "no" della Corte di giustizia alla data retention indiscriminata in campo penale*, in *Il diritto dell'informazione e dell'informatica*, 2, 2021, p.237.

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

42. Malacarne A.-Tessitore G., cit., p.25.

43. Rafaraci T., *Verso una law of evidence dei dati*, in *Diritto penale e processo*, 7, 2021, p.854.

44. Resta F., *La nuova disciplina dell'acquisizione dei tabulati*, in *Giustizia insieme,* 2021, pp. 2-3.

45. In questo senso Murro O., 2022, cit., p.2442.

46. Cassazione penale, Sezioni Unite, sentenza n. 21 del 13.07.1998. In banca dati *Dejure*.

47. Cassazione penale, Sezioni Unite., sentenza n. 6 del 23.02.2000, in banca dati *Dejure*.

48. Cassazione penale, Sezioni Unite., sentenza n. 16 del 21.6.2000, in banca dati *Dejure*.

49. In *https://giurcost.org*.

dati relativi all'identità dei soggetti ed ai riferimenti di tempo e di luogo di una comunicazione (in altri termini, i metadati) sono ricompresi nella garanzia apprestata dall'art. 15 Cost., ha concluso che le disposizioni sulle intercettazioni siano da riferire unicamente al contenuto delle conversazioni[50].

Pare lecito domandarsi se, di fronte alla possibilità di impiego delle nuove tecnologie dell'informazione e della comunicazione nella ricerca della prova ed all'avvento della telefonia digitale, costituisca un'operazione davvero giustificata quella di distinguere, quanto alle garanzie, in termini così netti intercettazione dei contenuti e acquisizione dei dati esterni.

Oggi relazioni ed attività di ogni tipo (lavoro, rapporti istituzionali ed interpersonali, ma anche attività illecite) si svolgono in gran parte *online*. La sociologa Deborah Lupton, ad evidenziare come le tecnologie digitali abbiano permeato la vita quotidiana delle persone che vivono nei paesi avanzati, ha intitolato "La vita è digitale" il primo capitolo di una propria opera[51]. In questo contesto, gli strumenti informatici hanno assunto il ruolo di vera e propria proiezione della più intima sfera della persona[52] . Ciò ha reso i dati della navigazione in Internet più significativi delle relazioni sociali svolte in forma fisica, con la conseguenza che il diritto alla riservatezza postula oggi una tutela rafforzata dei dati digitali[53]. In altre parole, il lato esposto dell'individuo nel mondo elettronico è aumentato incredibilmente, e ciò si rivela un ulteriore, grande vantaggio per chi ha intenzione di sorvegliarlo [54].

L'impatto di questo processo di digitalizzazione deve considerarsi dirompente anche rispetto al tema che ci occupa, non solo per la notevole capacità intrusiva dei nuovi mezzi di ricerca della prova, ma anche in ragione del fatto che, sul piano processuale, ad essi è comunemente attribuita, per loro stessa natura, una capacità euristica superiore a quella degli strumenti di prova tradizionali[55].

Quanto in particolare alla capacità intrusiva, in caso di acquisizione del duplicato di una strumentazione informatica sequestrata vi è il pericolo che gli investigatori entrino in contatto con una mole di dati non pertinenti al reato per cui si procede[56]. La giurisprudenza di legittimità[57] ha osservato che i sistemi informatici contengono una quantità innumerevole di dati e che nel corso delle indagini informatiche potrebbero essere acquisite anche informazioni "sensibili" e "supersensibili", relative alla sfera privata e intima dell'indagato[58]. Anche il cellulare ha perso, per il tramite della rete, la sua embrionale funzione meramente interlocutoria, di telefonare o messaggiare, per assumere la dimensione di un "nuovo luogo" al cui interno si dischiude un ambiente inedito ed impalpabile[59].

50. Secondo Torre sarebbe stato il mero dato letterale ad impedire l'estensione ai tabulati delle garanzie codicistiche e la Consulta non avrebbe ravvisato una differenza "qualitativa" tra i due mezzi probatori. Torre F., cit., p.542.

51. Lupton D., *Sociologia digitale*, Pearson, 2018, p.1.

52. Conti, C., *Sicurezza e riservatezza*, in *Diritto penale e processo*, 11, 2019, p.1574.

53. Tavassi L., *Acquisizione di tabulati, tutela della privacy e rispetto del principio di proporzionalità*, in *Archivio penale Web,* 2022*,* p.4.

54. Ziccardi G., *Sorveglianza elettronica, data mining e trattamento indiscriminato delle informazioni dei cittadini tra esigenze di sicurezza e diritti di liberta'*, in *Ragion pratica*, 1, 2018, p.36.

55. Malacarne A.-Tessitore G., cit., p.6.

56. Pittiruti M., *Dalla Corte di Cassazione un vademecum sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali omnibus*, in *Sistema penale*, 2021.

57. Corte di Cassazione, Sezione VI Penale, sentenza n. 34265 depositata il 2.10.2020, in *Sistema penale*, 2020.

58. Merita ricordare che, nell' accogliere il ricorso contro il sequestro probatorio del computer e dell'area server di una giornalista, la Corte di Cassazione (Sezione VI Penale, sentenza n. 40380 del 31.5.2007, in *Penale.it*) ha argomentato che la destinataria del provvedimento, peraltro non indagata, non poteva subire, a soli fini esplorativi, indiscriminate e pesanti intrusioni nella propria sfera privata attraverso l'acquisizione di tutto il materiale informatico posseduto ed attinente alla sua professione, ma doveva essere destinataria di un provvedimento "mirato". Recentemente la Suprema Corte (Cassazione Penale, Sez. VI, sentenza n. 17312 del 24.4.2024, in *Diritto penale e Processo*, 2024, n. 6, pp.763-764), al fine escludere misure con valenza meramente esplorativa, ha sancito, tra gli altri, il principio per cui è necessario che il Pubblico Ministero, quando dispone un sequestro esteso ed onnicomprensivo di un dispositivo informatico o telematico (nella specie uno *smartphone*), indichi nel decreto di sequestro: le ragioni per le quali è necessario disporre il sequestro in termini così ampi o, in alternativa, le informazioni oggetto della ricerca; i criteri che debbono presiedere alla selezione del materiale informatico archiviato nel dispositivo.

59. Murro O., *Prospettive in tema di sequestro dello smartphone: le novità approvate dal Senato*, in *Diritto penale e Processo*, 12, 2024, p. 1619. Peraltro, la Corte di Giustizia (Grande Sezione, sentenza del 4.10 2024, C-548/21, *CG contro Bezirkshaupt-*

Ma non si tratta solo di una questione quantitativa. Infatti, il *medium* informatico permette la genesi di dati che in passato sarebbero stati confinati nella mente, che l'individuo non intende condividere con alcuno e che diventano tuttavia "captabili"[60]. Comportamenti non comunicativi, o comunque non ancora comunicativi, divengono potenziale fonte di elementi probatori. Pertanto, i mezzi informatici di ricerca della prova possiedono una pervasività tale da aggredire non soltanto la riservatezza del domicilio fisico o di quello "informatico", ma potenzialmente persino l'inviolabilità della psiche umana[61]. Si pensi ad alcuni impieghi del "captatore informatico", quali il *keylogger* (captazione di tutto quanto viene digitato sulla tastiera), lo *screenshot* (fotografia di tutto ciò che appare sullo schermo del dispositivo controllato), lo *screencast* (videoregistrazione di ciò che passa sullo schermo del dispositivo bersaglio)[62]. Questa capacità di ottenere informazioni, è, diremmo esponenzialmente, accresciuta dal possibile ricorso all'intelligenza artificiale e agli strumenti di analisi predittiva, che sono stati definiti il fronte "caldo" delle indagini penali condotte con mezzi informatici[63]. A fronte dell' intrusività delle attività di indagine "informatiche", sembra peraltro criticabile il fatto che- in materia di ispezioni e perquisizioni informatiche, di sequestro di dati o sistemi, di accertamenti urgenti ad iniziativa della Polizia Giudiziaria sui sistemi- il nostro Codice di procedura penale non commini espressamente alcuna sanzione processuale per i casi di mancato rispetto delle tecniche e delle procedure (le *best practices*) idonee ad assicurare la corretta individuazione della fonte di prova digitale, ad impedire l'alterazione dei dati ed a garantire la conformità delle copie forensi all'originale, nonché la loro corretta conservazione[64]. Come noto infatti, errori nella raccolta o archiviazione dei dati digitali, dovuti a negligenza, mancanza di competenze o

mannschaft Landeck, in *dirittifondamentali.it*, 2024) ha statuito che, ai sensi della direttiva (UE) 2016/680 (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), una normativa nazionale che conceda alle autorità competenti la possibilità di accedere ai dati contenuti in un telefono cellulare a fini di prevenzione, ricerca, accertamento e perseguimento di reati in generale, deve definire in modo sufficientemente preciso la natura o le categorie dei reati in questione, garantire il rispetto del principio di proporzionalità e subordinare l'esercizio di tale possibilità ad un controllo preventivo di un giudice o di un organo amministrativo indipendente, salvo in casi di urgenza debitamente comprovati (§ 110). Inoltre, occorre informare gli interessati dei motivi sui quali tale autorizzazione si basa, a partire dal momento in cui ciò non rischia di compromettere le indagini condotte, e mettere a loro disposizione tutte le informazioni necessarie per consentire a tali persone di esercitare i propri diritti, in particolare il diritto di ricorso (§ 120). Tenuto conto di questa pronuncia, la Corte di Cassazione (Sezione sesta penale, sentenza n. 413 dell'8.4.2025, in *Sistema Penale,* 2025), in un caso di apprensione di dati personali contenuti in dispositivi elettronici mediante decreto del Pubblico Ministero, ha ritenuto che la normativa italiana non risponda alla previsione della direttiva (UE) 2016/680. Tuttavia, la Corte ritenuto che gli elementi acquisiti potessero essere utilizzati dal momento che, nel caso concreto, i diritti della difesa ad avere una valutazione giurisdizionale non erano stati pregiudicati, essendosi sul sequestro pronunciato il Tribunale per il riesame. Sulla questione si vedano Filippi L., *La CGUE mette i paletti all'accesso ai dati del cellulare*, in *Altalex*, 2024; Raucci P., *Le condizioni per l'accesso ai dati del cellulare per il diritto europeo*, in *Archivio penale Web*, 2, 2025; Malacarne, A., *La Cassazione sul sequestro dello smartphone: la disciplina italiana non è conforme al diritto dell'UE (… ma il materiale raccolto è comunque utilizzabile)*, in *Sistema penale,* 2025; Griffo M., *La Corte di cassazione fissa i criteri per il sequestro dei dati informatici e telematici (prima ed a prescindere dall'intervento del legislatore), in Giurisprudenza Penale Web, 6,* 2025.

60. Conti C., *Sicurezza e riservatezza*, in *Diritto penale e processo*, 11, 2019, p. 1574.

61. Conti C., *La corsa tecnologica tra Costituzione, codice di rito e norme sulla privacy: uno sguardo d'insieme*, in *Diritto penale e processo*, 6, 2021, p. 716.

62. Conti C., 2021, cit., p.721.

63. Conti C., 2021, cit., p.717. In merito all'utilizzo dell' IA nelle attività di prevenzione, accertamento, indagine e perseguimento di reati, basti qui citare il considerando n. 59 del Regolamento (Ue) 2024/1689 del 13.6.2024 sull'intelligenza artificiale (c.d. *AI Act*), secondo cui "*Tenuto conto del loro ruolo e della loro responsabilità, le azioni delle autorità di contrasto che prevedono determinati usi dei sistemi di IA sono caratterizzate da un livello significativo di squilibrio di potere e possono portare alla sorveglianza, all'arresto o alla privazione della libertà di una persona fisica, come pure avere altri impatti negativi sui diritti fondamentali garantiti nella Carta […] Potrebbe inoltre essere ostacolato l'esercizio di importanti diritti procedurali fondamentali, quali il diritto a un ricorso effettivo e a un giudice imparziale, nonché i diritti della difesa e la presunzione di innocenza, in particolare nel caso in cui tali sistemi di IA non siano sufficientemente trasparenti, spiegabili e documentati.*" L'utilizzo di sistemi di Intelligenza artificiale a fini di contrasto è disciplinato nel Regolamento specialmente dagli artt. 5, paragrafo 1, lettera h, e paragrafi 2,3,4,5,6.7, nonché all'art. 6 e dagli allegati II e III.

64. A parere di autorevole dottrina (Conti C., *La prova informatica e il mancato rispetto delle best practices*, in Cadoppi A.-Canestrari S.-Manna A.- Papa M. (diretto da), seconda edizione, Utet Giuridica, 2023, pp. 1542-1543), l'orientamento giurisprudenziale maggioritario, secondo il quale il valore dell'elemento di prova digitale acquisito senza rispettare le migliori pratiche è rimesso alla valutazione del giudice, conferisce all'organo giurisdizionale un'eccessiva discrezionalità. Perciò, la scelta in termini di inutilizzabilità dell'elemento di prova in tal caso risulterebbe preferibile, anche considerato che la modalità acquisitiva finisce per plasmare integralmente i contenuti della prova digitale in questione. Si è altresì sottolineato (Murro O., 2022, cit., p. 2454) come la riforma della *data retention* non abbia introdotto una completa disciplina concernente adeguate tecniche, finalizzate a garantire la corretta acquisizione dei dati, la loro conservazione e la formazione di una copia conforme e non modificabile.

metodologie inadeguate, possono compromettere la validità delle analisi e condurre a conclusioni erronee nel contesto del processo[65].

Molto significativa è la possibilità di ricavare informazioni anche dai dati esterni delle comunicazioni, la capacità di raccolta dei quali è aumentata grazie all'avvento della tecnologia digitale[66]. Si pensi, solo a titolo di esempio, ai metadati concernenti i siti web visitati. Di ciò è consapevole la Corte di Giustizia UE che, nelle pronunce sulla *data retention,* ha reiteratamente rilevato come "*i dati relativi al traffico e i dati relativi all'ubicazione possono rivelare informazioni su un numero significativo di aspetti della vita privata degli interessati, comprese informazioni delicate, quali l'orientamento sessuale, le opinioni politiche, le convinzioni religiose, filosofiche, sociali o di altro tipo nonché lo stato di salute*"[67]. La pregnanza di questi dati, destinati a confluire in enormi dataset, è resa ancora più evidente dalla possibilità di combinarli tra loro. Informazioni di per sé neutre, per effetto dell'impiego delle nuove tecnologie in grado di aggregare e di incrociare i dati stessi, possono comportare intromissioni indebite nella vita altrui[68]. La sentenza testè citata ha argomentato (sempre al paragrafo 61 e conformemente a numerosi altri precedenti) che "*Presi nel loro insieme, tali dati sono idonei a consentire di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono stati conservati, come le abitudini di vita quotidiana, i luoghi di soggiorno permanenti o temporanei, gli spostamenti giornalieri o di altro tipo, le attività esercitate, le relazioni sociali di dette persone e gli ambienti sociali da esse frequentati"*. I dati esterni delle comunicazioni non sono né statici, né"muti": possono essere correlati ad altri dati e fornire ulteriori informazioni. Non è importante soltanto il dato in sé, ma anche il metadato, ovvero il dato che si riferisce a un altro dato e, soprattutto, diventa fondamentale il nuovo dato che si genera correlando con algoritmi *ad hoc* dati preesistenti[69]. I cosiddetti dati esterni, dunque, offrono elementi di conoscenza eterogenei che trascendono il solo fatto storico dell'avvenuta comunicazione[70] e consentono di raccogliere plurime notizie sull'individuo, tali da delineare una mappatura esaustiva delle sue abitudini e tracciare un ritratto completo della persona[71]. Non si può neppure prevedere l'uso che dei dati prodotti oggi verrà fatto in futuro, grazie a nuovi strumenti di *data mining* e nuovi algoritmi, e non dovrebbe essere trascurato il fatto che è possibile, incrociando più dataset anche di fonti diverse, conferire un nome ed un cognome a dati in precedenza resi anonimi[72].

Ciò posto, la distinzione tra (maggiore) invasività delle intercettazioni e (minore) invasività dell'acquisizione dei metadati ha perso probabilmente gran parte della propria ragion d'essere. In questo senso si è osservato come, con il perfezionarsi della tecnologia, non si possa aprioristicamente stabilire se l'acquisizione dei tabulati sia meno invasiva rispetto all'apprensione del contenuto di una conversazione[73] e che la "profilazione" resa possibile dai metadati rappresenti, secondo la stessa Corte di Giustizia UE, un'informazione tanto delicata, quanto il contenuto stesso della comunicazione[74]. E'stato anzi considerato come i tabulati possano contenere dati più significativi delle conversazioni, nelle quali non è inusuale l'utilizzo di linguaggi cifrati o che si presti molta attenzione[75] e, aggiungiamo, nelle quali potrebbero persino essere espresse mere vanterie. Quanto al

65. Croci L., *La Corte Penale Internazionale e le prove digitali. Gestione, sfide e innovazioni nell'era digitale*, in questa rivista, 18 (1), 2025, pp.4-5.

66. Corte Suprema di Cassazione. *Relazione su novità normativa. 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)*, n.55 del 2021, in *https://www.cortedicassazione.it*, p .7.

67. Corte di Giustizia, Grande Sezione, sentenza del 20.9.2022, *SpaceNet AG e Telekom Deutschland GmbH,* paragrafo 61 e giurisprudenza ivi citata.

68. Baccari G.M., cit., p.1869.

69. Ziccardi G., 2018., cit., p.31.

70. Tavassi L., cit, p.2.

71. Murro O., 2022, cit., p.2443.

72. Cfr. Lupton D., op. cit., p. 116.

73. Torre F., 2021, cit. pp.551-552.

74. Tartara V., *La Corte di Giustizia conferma il "divieto di conservazione generalizzata e indiscriminata" dei dati relativi al traffico delle comunicazioni elettroniche per finalità preventive di contrasto alla criminalità. Possibili ricadute nell'ordinamento italiano*, in *Sistema penale,* 2022, p. 185.

75. Malacarne A.-Tessitore G., cit., p.10.

grado di lesione del diritto alla riservatezza, non è di poco conto evidenziare che la *data retention* presenta, rispetto all'intercettazione, l'attitudine a comportare la conservazione "preventiva" di dati di un numero di persone potenzialmente molto più ampio di quelli effettivamente utili alle indagini penali[76]. In ultima analisi, sembra da condividersi l'opinione[77] secondo cui la tradizionale suddivisione tra dati esterni e contenuto della comunicazione meriti un ripensamento. La suddivisione è forse divenuta persino anacronistica.

A fronte di queste considerazioni si potrebbero prospettare due diverse opzioni.

La prima consiste nell'incremento delle garanzie per l'acquisizione dei dati esterni delle comunicazioni telefoniche e telematiche e dei dati di ubicazione, nell'ottica di un avvicinamento alle regole delle intercettazioni di conversazioni e così anche di un adeguamento all'evoluzione delle tecnologie digitali, il cui uso nel procedimento penale deve essere, per quanto detto sopra, ben perimetrato. Questa sembra essere la strada percorsa nel 2021 dal legislatore con la parziale riscrittura dell'art. 132 D.lgs. n.196 del 30.6.2003. Come anticipato sommariamente al § 2, il comma 3 dell'odierna disposizione richiede, per la legittimità della procedura di acquisizione, la ricorrenza di sufficienti indizi di reati tassativamente individuati (in base alla pena edittale o in via nominativa), che i dati siano rilevanti per l'accertamento dei fatti, e che vi sia l'autorizzazione rilasciata da un giudice con decreto motivato (su richiesta del Pubblico Ministero o istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private); il comma 3 bis, contempla una procedura d'urgenza, nella quale il provvedimento di convalida del giudice deve comunque intervenire entro termini perentori; il comma 3-quater dispone l'inutilizzabilità dei metadati acquisiti in violazione delle disposizioni procedurali previste[78]. La differenza, dal punto di vista dei requisiti formali e sostanziali, tra acquisizione dei dati esterni e intercettazione di comunicazioni o conversazioni si è dunque assottigliata, senza però scomparire del tutto. I requisiti richiesti dall'art. 132 D.lgs. n.196 del 30.6.2003 restano infatti meno stringenti rispetto a quelli necessari per procedere alle intercettazioni: gli indizi di reato debbono essere "sufficienti" anziché "gravi"[79]; il catalogo dei reati che consentono l'acquisizione dei metadati è più ampio di quello delle intercettazioni; ai sensi dell'art. 132 è richiesta la "rilevanza" dei metadati per l'accertamento dei fatti (anziché l'assoluta indispensibilità); nei casi d'urgenza, il termine concesso al Pubblico Ministero per la trasmissione del decreto di acquisizione al giudice è più lungo (quarantotto ore anziché ventiquattro). Inoltre, nel silenzio della novella, non risulta riconosciuto, a differenza di quanto accade per le intercettazioni, il diritto dell'imputato alla distruzione dei tabulati acquisiti illegalmente, con una conseguente disparità di trattamento tra l'imputato soggetto ad intercettazioni illegali e l'imputato soggetto ad acquisizione di tabulati illegale[80] .

In ragione della considerevole capacità dei metadati di rivelare informazioni personali, potrebbe esservi un'altra opzione per il legislatore: quella dell'estensione alla *data retention* di tutte le regole di cui alle disposizioni concernenti intercettazioni di conversazioni o comunicazioni. Ciò nella misura in cui tali disposizioni siano compatibili con la natura della *data retention* medesima -la quale comporta, come noto, l'acquisizione dei metadati *dopo* la comunicazione o la conversazione- e con esclusione, ad esempio, delle disposizioni che presuppongono necessariamente la compresenza degli interlocutori e la contestualità della comunicazione o delle recenti disposizioni sulla durata massima delle operazioni di intercettazione.

76. Flor R.-Marcolini S., op. cit., pp.46-47.

77. Corte Suprema di Cassazione. *Relazione su novità normativa. 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*), n.55 del 2021, p .7.

78. Comportano l'inutilizzabilità dei dati ex art. 132, c. 3-quater l'acquisizione oltre il termine di conservazione, l'autorizzazione conferita per un reato non previsto, l'assenza di una motivazione specifica sulla qualificazione giuridica, sui "sufficienti indizi di reato" o sulla loro rilevanza per l'accertamento dei fatti. Filippi, L. 2022, *Riservatezza e data retention: una storia infinita*, cit. La Corte di Cassazione (Sezione seconda penale, sentenza n. 18840 depositata il 20.5.2025, in *https://canestrinilex.com*) ha ritenuto totalmente ed assolutamente inutilizzabili i dati relativi al traffico telefonico acquisiti dal Pubblico ministero senza la previa autorizzazione o la successiva convalida del giudice competente.

79. "Sufficienti" indizi possono, ai sensi del D.L. n. 152 del 13.5.1991, convertito in legge con modificazioni dalla L. n. 203 del 12.7.1991 (come novellato L. n. 90 del 28.6.2024, *"Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici"*), legittimare le intercettazioni solo per fatti di criminalità organizzata e per i reati informatici rimessi al coordinamento del Procuratore nazionale Antimafia ed Antiterrorismo.

80. Giangreco M., *Data retention*, *acquisizione e utilizzabilità dei tabulati telefonici e telematici: una riflessione incrociata*, in *Cassazione penale*, 4, 2022, p.1686.

A sostegno di una completa parificazione normativa tra intercettazioni ed acquisizione dei dati esterni, può essere evidenziata l'affermazione della Corte di Giustizia UE[81], secondo cui i dati relativi al traffico o i dati relativi all'ubicazione conservati forniscono i mezzi per consentire il profilo della persona o delle persone interessate e che ciò rappresenta un'informazione tanto delicata, alla luce del rispetto della vita privata, quanto il contenuto stesso delle comunicazioni. Una considerazione di analogo tenore è stata formulata anche dalla Corte Europea per i diritti dell'uomo[82], che si è espressa nel senso di un'equiparazione tra la gravità dell'ingerenza attuata mediante l'acquisizione di dati esterni alla comunicazione e di quella costituita dalla captazione del loro contenuto.

In questo senso, di grande rilevanza appaiono altresì le argomentazioni svolte in due pronunce della nostra Corte Costituzionale, che segnano un ulteriore mutamento di sensibilità quanto all'inquadramento giuridico degli atti investigativi "tecnologici". La prima è rappresentata dalla sentenza della Corte Costituzionale n. 38 del 23.1.2019[83]. Nella specie era stata sollevata questione di legittimità costituzionale -per violazione dell'art. 68, comma 3, della Costituzione- dell'art. 6, comma 2, della legge 20.6.2003 n. 140, recante *"Disposizioni per l'attuazione dell'articolo 68 della Costituzione nonché in materia di processi penali nei confronti delle alte cariche dello Stato"*, nella parte in cui prevede che il giudice chieda alla camera, alla quale il parlamentare appartiene o apparteneva, l'autorizzazione anche all'utilizzo dei tabulati telefonici acquisiti a carico di terzi. Il giudice rimettente aveva osservato che nell'art. 68, comma 3, Cost. non compare alcun riferimento ai tabulati. Nel dichiarare non fondata la questione di legittimità della legge, la Consulta ha, tra l'altro, ritenuto non condivisibile il presupposto secondo cui tra il contenuto di una conversazione o di una comunicazione, da un lato, e il documento che rivela i dati estrinseci di queste, dall'altro, sussisterebbe una differenza "ontologica" ed ha invece concluso che il duplice riferimento, nell'art. 68, comma 3, Cost. a "conversazioni o comunicazioni" induca a ritenere che al contenuto di una comunicazione siano accostabili anche i dati storici ed esteriori, in quanto essi stessi "fatti comunicativi". Non sarebbe prudente ravvisare in questa pronuncia un *revirement* rispetto alle sentenze citate all'inizio di questo paragrafo. Tuttavia, può quantomeno dirsi che essa non sembra chiudere all'opzione qui considerata. Peraltro, nella prospettiva di un'equiparazione tra i due mezzi di ricerca della prova, potrebbe ritenersi non ultronea la presenza, nella recente riforma della *data retention,* di una norma che ha modificato anche l'istituto delle intercettazioni mediante il captatore informatico[84]. E che rappresenta quasi un ideale ponte tra tabulati ed intercettazioni.

Un'estensione delle garanzie costituzionali delle comunicazioni effettuate tramite le tecnologie digitali in genere è stata operata anche dalla sentenza della Corte Costituzionale n. 170 depositata il 20.7.2023[85]. La sentenza ha concluso che l'art. 68, comma 3, Cost. tutela la corrispondenza dei membri del Parlamento, compresa quella elettronica, anche dopo la ricezione da parte del destinatario, almeno fino a quando, per il decorso del tempo, essa non abbia perso ogni carattere di attualità in rapporto all'interesse alla sua riservatezza. Nella specie trattavasi di messaggi di posta elettronica e *WhatsApp.* Nelle proprie argomentazioni la Consulta ha respinto la tesi (peraltro fino ad allora consolidata nella giurisprudenza della Corte di Cassazione) secondo cui la corrispondenza già ricevuta e letta dal destinatario non sarebbe più un mezzo di comunicazione, ma un semplice documento (non coperto dalla garanzia costituzionale in questione). Infatti, detta tesi, secondo il giudice delle leggi, finirebbe addirittura per azzerare, di fatto, per le comunicazioni tramite posta elettronica o servizi di messaggeria istantanea, la tutela prefigurata dall'art. 15 Cost, atteso che in tali comunicazioni all'invio segue immediatamente, o comunque senza uno iato di tempo apprezzabile, la ricezione[86]. Il progresso tecnologico

81. Da ultimo, con la più volte citata sentenza della Grande Sezione del 20.9.2022, *SpaceNet AG e Telekom Deutschland GmbH,* § 87.

82. Corte Europea dei diritti dell'uomo, sentenza del 13.9.2018, *Big Brother Watch ed altri contro Regno Unito,* § 363*,* in *www.hudoc.echr.coe.int* .

83. In *https://www.cortecostituzionale.it.*

84. Con l'art. 1, comma 1-ter, D.L. n. 132 del 30.09. 2021, convertito, con modificazioni, dalla L. n. 178 del 23.11.2021, (*"Al terzo periodo del comma 1 dell'articolo 267 del codice di procedura penale, le parole: "indica le ragioni" sono sostituite dalle seguenti: "indica le specifiche ragioni"*).

85. In *Giurisprudenza penale Web*, 7-8, 2023.

86. Il *dictum* della Corte Costituzionale è stato recepito dalla sentenza della Corte di Cassazione, Sezione VI penale, n. 31180 del 30.7.2024 (in *https://www.cortedicassazione.it*), secondo la quale non solo le chat costituiscono corrispondenza informatica, ma il principio affermato dal giudice delle leggi ha portata generale e non si riferisce esclusivamente all'ambito applicativo dell'art. 68 Cost. sulle guarentigie prestate a favore del parlamentare.

impone di adeguare concetti e garanzie ad un contesto storico in cui forme di comunicazione, da un lato, e strumenti investigativi, dall'altro, sono in costante e rapida evoluzione[87]. Potrebbe dirsi che il *discrimen* tra i mezzi di ricerca della prova sia divenuto più incerto. In questa direzione si è osservato che l'evoluzione tecnologica nel campo delle comunicazioni digitali ha ridimensionato, depotenziandola, l'importanza della differenza tra comunicazione sincrona e asincrona, che sta alla base della tradizionale distinzione codicistica tra sequestro della corrispondenza e intercettazione delle comunicazioni[88]. Anche la distinzione tra intercettazioni a mezzo del captatore informatico e perquisizioni *online* appare connotata da un'ampia *gray area*, dovuta alle tecniche con le quali si procede, di volta in volta, all'applicazione del programma[89].

Ancora, si potrebbe sottolineare come i reati per i quali è consentita l'intercettazione siano meno numerosi e in genere più gravi rispetto a quelli che possono attualmente legittimare l'acquisizione dei metadati. Limitare anche l'ammissibilità di quest'ultima al novero delle fattispecie elencate nell'art. 266 c.p.p. renderebbe l'istituto della *data retention* più conforme al principio, come si è visto sancito (anche) dalla sentenza H.K., secondo cui l'accesso di autorità pubbliche ad un insieme di dati relativi al traffico o di dati relativi all'ubicazione -che siano idonei a fornire informazioni sulle comunicazioni effettuate da un utente o sull'ubicazione delle apparecchiature terminali utilizzate e a permettere di trarre precise conclusioni sulla sua vita privata- deve essere circoscritto alla lotta contro le "forme gravi di criminalità" o alla prevenzione di "gravi minacce alla sicurezza pubblica".

Una normativa con minori garanzie, e perciò più agile rispetto a quella concernente le intercettazioni, potrebbe essere riservata alla conservazione e all'acquisizione dei dati esterni ritenuti meno "pericolosi" dalla Corte di Giustizia[90], come gli indirizzi IP e quelli relativi all'identità anagrafica degli utenti, se conservati in modo da non consentire una profilazione. In questa direzione può considerarsi che, secondo la CGUE[91], l'accesso a dati relativi all'identità civile degli utenti dei mezzi di comunicazione elettronica - al solo scopo di identificare l'utente considerato e senza che tali dati possano essere associati a informazioni relative alle comunicazioni effettuate- non integra, in linea di principio, un'ingerenza grave. In tale ipotesi, secondo la Corte, il requisito di un previo controllo da parte di un giudice o di un organo amministrativo indipendente non sarebbe applicabile. Se ne può probabilmente trarre la conseguenza che sia da considerarsi ammissibile, ed anche per reati non gravi, un'acquisizione di tali metadati con provvedimento del Pubblico Ministero.

5 …e garanzia dei diritti

Le tecnologie informatiche sono, si è cercato di evidenziare, dotate di un potenziale molto rilevante di invasività e, di conseguenza, di impatto sui diritti fondamentali. La capacità intrusiva dei mezzi di indagine che progressivamente si rendono disponibili per lo Stato investigatore sviluppa in modo direttamente proporzionale la naturale tensione tra espansione dei diritti dell'individuo e necessità di prevenzione e accertamento di fatti di reato[92]. E'stato in proposito scritto che il tema della sorveglianza tecnologica, pervasiva e contemporaneamente non percepibile, rappresenta uno dei principali punti di attrito rispetto alla protezione dei diritti umani[93].

Ciò vale anche per la sorveglianza effettuata attraverso l'istituto della *data retention*, che comporta il trattamento automatizzato di enormi quantità di dati e pone innanzi tutto una questione di tutela dei diritti alla riservatezza della vita privata ed alla protezione dei dati personali. La raccolta, la conservazione e l'accesso a tutti questi dati integrano, sotto questo profilo, anche un pericolo di dossieraggio[94] .

87. Fontani C., *La svolta della Consulta: la "corrispondenza telematica" è pur sempre corrispondenza*, in *Diritto penale e processo,* 10, 2023, p.1322.

88. Torre M., *Considerazioni su perquisizione, sequestro e intercettazioni digitali*, in *Diritto penale e processo,* 6, 2024, p.812.

89. Flor R.-Marcolini S., op. cit., p. 136.

90. Vedi retro, §3.

91. Già citata (supra, § 3) sentenza CGUE, Grande camera, del 30.4.2024 (causa c-470/21, La Quadrature du Net ed altri.) §§ 131-134.

92. Leo G., *Le indagini sulle comunicazioni e sugli spostamenti delle persone: prime riflessioni riguardo alla recente giurisprudenza europea su geolocalizzazione e tabulati telefonici*, in *Sistema penale,* 2021, p.1.

93. Perri P., *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, Giuffré Francis Lefebvre, 2020, p. 135.

94. Murro O., 2022, cit., p. 2454.

La conservazione e l'accesso ai dati del traffico per fini di prevenzione e repressione di reati e di sicurezza pubblica, incidono altresì sulla libertà di espressione. Ad esempio, studi empirici effettuati dopo il caso *Snowden* hanno consentito di rilevare una diminuzione di ricerche effettuate mediante l'uso di termini potenzialmente compromettenti, come "aborto" e "terrorismo", ed hanno condotto gli autori degli studi ad ipotizzare una connessione tra la diminuzione di queste attività di ricerca e meccanismi di autoinibizione dovuta alla consapevolezza di essere osservati *online*[95]. La questione è ben presente nella riflessione della Corte di Giustizia UE, la quale ha ritenuto[96] che "[…] *la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione a fini di polizia è idonea a ledere il diritto al rispetto delle comunicazioni, sancito dall'articolo 7 della Carta, e a comportare effetti dissuasivi sull'esercizio, da parte degli utenti dei mezzi di comunicazione elettronica, della loro libertà di espressione, garantita dall'articolo 11 della Carta, effetti che sono tanto più gravi quanto maggiori sono il numero e la varietà dei dati conservati*". L'ordinamento giuridico non può permettere che l'individuo rinunci ad avvalersi delle tecnologie digitali perché si sente sorvegliato[97].

La sorveglianza digitale implica inoltre rischi per l'autonomia individuale, la libertà di partecipazione alla vita politica, il principio di non discriminazione[98]. Il Regolamento europeo sull'Intelligenza Artificiale (Regolamento UE 2024/1689 del 13.6.2024, Considerando n.32) osserva, a proposito dell'uso di sistemi di IA di identificazione biometrica remota in tempo reale delle persone fisiche, in spazi accessibili al pubblico ed a fini di attività di contrasto, che tale uso potrebbe fare sentire un'ampia fetta della popolazione costantemente sotto sorveglianza e scoraggiare in maniera indiretta anche l'esercizio della libertà di riunione.

Come noto, nella concezione propria del costituzionalismo contemporaneo i diritti vengono sottratti all'influenza diretta del potere politico, affermati come antecedenti l'autorità dello Stato e costituiscono principi giuridici superiori alla capacità di normazione dell'autorità statuale[99]. In questa prospettiva, le norme di diritti fondamentali presentano una fondamentalità formale, in quanto -per la loro posizione di vertice nell'ordinamento giuridico- costituiscono un diritto immediatamente vincolante il potere legislativo, il potere esecutivo ed il potere giudiziario[100]. Inoltre, diritti fondamentali e norme di diritti fondamentali rivestono una fondamentalità materiale, perché con essi si prendono decisioni sulla struttura normativa di base dello Stato e della società[101]. La tutela dei diritti si è peraltro evoluta verso la "nuova frontiera" rappresentata dall'ingresso del diritto internazionale e soprattutto, per quanto concerne l'ambito europeo, dall'introduzione della Carta dei diritti dell'Unione europea e dall'entrata in vigore della Convenzione europea dei diritti dell'uomo e delle libertà fondamentali[102]. Lo Stato costituzionale si è aperto alla dimensione dell'ordine giuridico sovranazionale, mediante la cessione di quote della sovranità[103]. Negli odierni sistemi i diritti fondamentali integrano pertanto i parametri di valutazione degli ordinamenti e la legittimazione di istituzioni e norme giuridiche dovrebbe svolgersi attraverso argomentazioni formulate a partire da diritti e libertà. In questo senso, la libertà è quella situazione rispetto alla quale l'autorità deve giustificare sé stessa[104].

Con riguardo alle banche dati (sia quelle centralizzate, sia quelle decentralizzate a livello di Stati membri) attraverso le quali in ambito Ue le autorità pubbliche esercitano il controllo della criminalità e dei confini, è stato considerato che la sorveglianza digitale europea si sta espandendo nella direzione di una crescente circolarità ed autoreferenzialità delle iniziative adottate[105]. Con tale affermazione evidenziando che le giustificazioni

95. Orrù E., cit., p.240.

96. Nella già menzionata sentenza della Grande sezione del 5.4.2022 (*G.D.* contro *Commissioner of An Garda Síochána* ed altri) § 46 e giurisprudenza ivi citata.

97. Conti C., 2019, cit., p.1575.

98. Orrù E., op. cit., p.241.

99. Bongiovanni G., *Diritti inviolabili e libertà*, in Barbera, A. (a cura di). *Le basi filosofiche del costituzionalismo*, Laterza, 2019, p. 86.

100. Alexy R., *Teoria dei diritti fondamentali*, Il Mulino, 2012, p.551.

101. ibidem., p.553.

102. Caretti P.- Tarli Barbieri G., op. cit., p.14.

103. Omaggio V., *Ascesa e declino della democrazia costituzionale*, in *Rivista di Filosofia del Diritto*, 2, 2024, p.379.

104. La Torre M.- Zanetti G., *Seminari di Filosofia del diritto*, Rubbettino, 2000, p.78.

105. Orrù E., cit., p. 238.

poste alla base dell'introduzione di nuove banche dati tendono a fare ricorso ad argomenti autoreferenziali, in base ai quali le nuove misure di sorveglianza non si fondano sulla necessità di fare fronte ad eventi esterni (come un effettivo aumento della criminalità), ma sulla mera esigenza di colmare le lacune presenti nei sistemi preesistenti. Argomenti di questo tipo presentano una "tendenza espansiva in sé non limitabile, dal momento che, al di fuori di un sistema di sorveglianza totale, l'esistenza di lacune è inevitabile"[106] e, pertanto, non rappresentano un buon esempio di ragionamento "a partire dai diritti", prestandosi a legittimare -in ragione dell'incessante e rapidissima evoluzione delle tecnologie digitali- la pressocché continua implementazione di nuove banche dati a scopo di sorveglianza. E ciò per il solo motivo di poterlo fare tecnicamente. Evidenti criticità presentava anche la normativa italiana sulla *data retention* precedente la riforma del 2021. Si trattava di una disciplina rimodulata e rafforzata dopo i numerosi attentati che si sono susseguiti in Europa dal 2005 in poi, con il risultato di sbilanciare la norma sulla tutela delle esigenze di difesa sociale in danno dei diritti fondamentali dell'individuo[107], e che non operava alcun effettivo bilanciamento tra diritti fondamentali ed esigenza di accertamento di gravi reati[108]. Tanto è vero che il legislatore dopo la pronuncia della sentenza H.K. ha ravvisato la necessità e l'urgenza di porre mano all'art.132 D.lgs. n.196 del 30.6.2003.

Come si è visto sinora, nella giurisprudenza della CGUE quello di proporzionalità rappresenta il criterio principale attraverso cui ricercare il delicato equilibrio tra la salvaguardia dei diritti fondamentali ed il perseguimento da parte delle pubbliche autorità di finalità legittime (quali, ad esempio, l'accertamento dei reati, la salvaguardia della sicurezza pubblica e la sicurezza nazionale). L'attività di sorveglianza può svolgere un ruolo impagabile di prevenzione rispetto ad eventi tragici, ma occorre trovare un modo per disciplinarla, soprattutto in ragione dell'apporto tecnologico che ha reso possibili operazioni finora inimmaginabili[109]. Secondo la sentenza H. K., in virtù del requisito della proporzionalità le deroghe alla protezione dei dati personali e le limitazioni di quest'ultima devono compiersi entro i limiti dello stretto necessario (§ 38). Con la sentenza *SpaceNet AG*[110] la Corte di Giustizia ha ricordato- circa la tutela del diritto fondamentale alla vita privata e le deroghe e restrizioni alla tutela dei dati personali- che un obiettivo di interesse generale non può essere perseguito senza tenere conto del fatto che esso deve essere conciliato con i diritti fondamentali interessati dalla misura, effettuando un contemperamento equilibrato tra l'obiettivo di interesse generale e i diritti di cui trattasi. Il che vale ovviamente non solo per il diritto alla protezione dei dati personali, ma per tutti i diritti fondamentali, come di evince dai più volte citati art. 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione Europea e art. 15, paragrafo 1, della Direttiva 2002/58/CE[111]. E con la precisazione[112] che, anche in caso di bilanciamento, il nucleo essenziale del diritto fondamentale non deve essere compromesso. Il rispetto della proporzionalità comporta a nostro avviso che la sorveglianza digitale per fini istituzionali non possa in ordinamenti liberaldemocratici perseguire il "rischio zero", cioè una sicurezza in senso assoluto, in quanto ciò si realizzerebbe inevitabilmente attraverso un'attività di sorveglianza pressoché illimitata ed al costo dei diritti, quantomeno nei termini di un loro svuotamento di fatto. Una società sotto sorveglianza non è più una democrazia, inoltre la sorveglianza di massa tratta ogni cittadino alla stregua di un potenziale sospetto e sovverte la presunzione di innocenza[113]. Non va, per inciso, dimenticato che l'anonimato sul web può rapp-

106. Orrù E., cit., p.239.

107. Murro O., 2022, cit., p.2442.

108. Rinaldini F., *Data retention e procedimento penale. Gli effetti della sentenza della Corte di Giustizia nel caso H.K. sul regime di acquisizione dei tabulati telefonici e telematici: urge l'intervento del legislatore*, in *Giurisprudenza Penale Web*, 5, 2021, p.8.

109. Perri P., op. cit., p. 129.

110. Corte di Giustizia, Grande Sezione, sentenza del 20.9.2022 (cause riunite C-793/19 e C-794/19), § 67 e giurisprudenza ivi citata.

111. Il rispetto dei diritti fondamentali, nonché dei principi di necessarietà e proporzionalità, è richiesto anche dalla Direttiva (UE) 2016/680 del 27.4.2016, 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 (recepita dall' Italia con il D.lgs. n. 51 del 18.5.2018). Con la sentenza della Grande Sezione del 4.10.2024 (causa C-548/21, *CG* contro *Bezirkshauptmannschaft Landeck, in Archivio penale web,* 2024) la Corte di Giustizia ha avuto modo di precisare che, ai sensi dell'articolo 4, paragrafo 1, lettera c) della direttiva (UE) 2016/680, gli Stati membri devono prevedere che i dati personali siano adeguati, pertinenti e non eccessivi rispetto alle finalità per le quali sono trattati. E che tale disposizione richiede quindi il rispetto, da parte degli Stati membri, del principio di «minimizzazione dei dati», il quale dà espressione al principio di proporzionalità (§79).

112. Conti C., 2019, cit., p. 1578.

113. *Contro i sistemi di sorveglianza: appello di 560 scrittori ed intellettuali*, in Rodotà S., *Il mondo nella rete. Quali i diritti, quali*

resentare, in paesi sottoposti a regimi autoritari, una forma di protezione per coloro che vogliono esprimere la propria opinione o battersi in difesa dei diritti umani[114]. Perciò, l'ordinamento dovrebbe tendere, più ragionevolmente, a contenere il rischio di commissione di reati e di impunità dei loro autori, riducendolo ad un rischio (soltanto) "sopportabile", cioè ridotto entro una dimensione di accettabilità sociale, perseguibile attraverso norme giuridiche in grado di coesistere con le libertà costituzionali.

L'emanazione di normative non rispettose dei diritti soggettivi e del principio di proporzionalità pone ovviamente questioni rilevanti. E' vero, da una parte, che tali normative sono sottoponibili ad un controllo giudiziario che può condurre anche ad una loro invalidazione, come avvenuto per la Direttiva europea "Frattini" sulla *data retention* nel 2006. Ma, dall'altra, ciò rappresenta un rimedio parziale e non sempre adeguato alla protezione dei diritti. Invero, il controllo giudiziario è uno strumento *ex post*, con la conseguenza che nel periodo di tempo intercorrente tra l'emanazione della norma e l'accertamento della sua incompatibilità con i diritti fondamentali questi vengono inevitabilmente violati[115]. Si potrebbe aggiungere a quanto sopra una considerazione. L'approvazione di leggi non adeguatamente "calibrate" sui diritti può contribuire ad innalzare la soglia di tolleranza da parte dei consociati verso pratiche di sorveglianza elettronica, persino se non proporzionate, generando o comunque alimentando argomenti che non sono *rights-based*, con un effetto di dis-educazione alla cittadinanza digitale. Ad esempio, si pensi all'assunto secondo il quale non ci si dovrebbe opporre alla sorveglianza se non si ha nulla da nascondere o quello[116] secondo cui di fronte al bisogno di combattere le diverse forme di criminalità tutto sia consentito alle autorità preposte alla tutela della collettività. Tali argomenti, non fondati sui diritti, possono diffondersi nella mentalità comune, trovare uno spazio nel dibattito pubblico e persino talora insinuarsi nelle pieghe di discorsi dei giuristi. E non paiono sempre facili da eradicare, neppure attraverso pronunce delle massime giurisdizioni nazionali o sovranazionali, o perché sarebbe necessario lo scrutinio di tutte le fonti che recano norme concernenti la sorveglianza digitale[117], oppure per possibili resistenze nella stessa giurisprudenza successiva. In altri termini, una legislazione poco sensibile alle esigenze di equilibrio tra sicurezza pubblica e libertà può rendere l'ecosistema giuridico sempre meno propizio al recepimento del linguaggio dei diritti e, di conseguenza, i ragionamenti in favore di diritti e libertà più "faticosi".

Una "fatica dei diritti" è probabilmente ravvisabile nell'interpretazione fornita dalla nostra giurisprudenza di legittimità dell'art.132 D.lgs. n.196 del 30.6.2003 prima della riforma del 2021. Con un orientamento consolidato, la Corte di Cassazione si era pronunciata -nonostante i numerosi input provenienti dalla Corte di Giustizia Ue a partire dalle sentenze *Digital Rights Ireland* e *Tele2 Sverige*- a favore della conformità dell'art. 132 al diritto sovranazionale in materia di privacy. La Suprema Corte, con la sentenza della Sezione quinta penale n. 33851 del 24.4.2018,[118] aveva infatti ritenuto che le sentenze *Digital Rights* e *Tele 2* riguardassero Stati privi, a differenza dello Stato italiano, di una regolamentazione dell'accesso e della conservazione dei dati personali. Nella medesima sentenza è stato altresì concluso che fosse del tutto legittima l'attribuzione del potere di acquisizione dei dati al pubblico ministero, in quanto il termine "giudice" di cui alle sentenze CGUE (che richiedono, come visto, un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente) doveva essere inteso nel senso esteso di "autorità giudiziaria", comprensivo della figura del pubblico ministero. Ricavando ciò anche dal termine *jurisdiction* utilizzato nella versione francese delle predette sentenze della Corte di Giustizia, che è riferibile alla magistratura francese nel suo complesso (composta da

i vincoli, Laterza, 2014, p.98.

114. Cfr., Masera A.-Scorza G., *Internet, i nostri diritti*, Laterza, 2016, p.55.

115. Orrù E., cit., p.243.

116. La Rocca E.N., *A margine di una recente sentenza della Corte di giustizia UE (c-748/18): riflessi sinistri sulla disciplina delle intercettazioni in Italia*, in *Diritti Comparati*, 1, 2021, p.1.

117. Tra le fonti non ancora qui citate, si pensi alla Direttiva (UE) 2016/681 del 27.4.2016 sull'uso dei codici di prenotazione aerei (PNR) a fini di prevenzione, accertamento, indagine e repressione di reati di terrorismo e di altri gravi reati, recepita dall'Italia con il D.L.gs. n. 53 del 21.5.2018. La Corte di Giustizia ha avuto modo di osservare che anche la Direttiva PNR comporta un'ingerenza grave nei diritti alla riservatezza e alla protezione dei dati personali, nella misura in cui mira a istituire un sistema di sorveglianza continua, indiscriminata e sistematica, che include la valutazione automatizzata di dati personali di tutte le persone che utilizzano sistemi di trasporto aereo. Si veda Càrpino M., *Il trattamento dei dati personali per finalità di prevenzione, indagine, accertamento e perseguimento di reati*, Giappichelli, 2024, p.215.

118. In banca dati *Dejure*.

giudici e pubblici ministeri), e dal termine *Court* adottato nella versione inglese, considerato promiscuo e differente da quelli più precisi di giudice (*judge*) e pubblico ministero (*prosecutor*). Questi passaggi sono stati ribaditi dalla successiva sentenza della Sezione terza penale n. 66380 del 19.4.2019[119], che aveva altresì giudicato la soluzione italiana coerente con il sistema di tipo accusatorio, anche considerato che l'acquisizione del dato del traffico generebbe una compromissione decisamente inferiore rispetto a quella relativa alla captazione delle conversazioni, affidata al controllo del giudice per le indagini preliminari. Sulla stessa linea si è posta la sentenza della Sezione terza, n. 46737 del 25.09. 2019[120], secondo la quale inoltre il giudizio di proporzionalità -richiesto dalla Corte di giustizia per procedere legittimamente alla conservazione e all'acquisizione dei dati esterni delle comunicazioni- si sarebbe potuto effettuare, pur in mancanza di una disposizione che limitasse l'accesso ai dati a categorie di reati ritenuti particolarmente gravi, in base a criteri di valutazione ricavabili tra gli altri dall'art. 266 c.p.p. (riguardante i reati per i quali sono ammesse intercettazioni). La legittimità dell'art. 132 era stata infine sostenuta dalla sentenza della Sezione seconda, n. 5741 del 10.12.2019[121], che aveva attinto in sostanza alle ragioni già espresse nei precedenti della Suprema Corte[122].

Tale orientamento ha ricevuto critiche. Si è parlato in proposito di "un'occasione mancata per prendere i diritti davvero sul serio"[123], di "tecniche argomentative acrobatiche" volte a salvare la disciplina interna e di "fantasia argomentativa"[124], di posizioni della giurisprudenza interna non irrobustite dal confronto con i diritti della persona riconosciuti dalla normativa sovranazionale[125], di un atteggiamento di chiusura dell'organo nomofilattico[126]. In questo senso è stato eccepito, tra l'altro: che non solo non risponde a realtà che le sentenze *Digital Rights* e *Tele2* avrebbero riguardato Stati privi di una regolamentazione in materia, ma anche che i giudici di Strasburgo avevano stabilito una serie di principi universalmente validi, non legati alla normativa di un singolo ordinamento giuridico[127]; che la considerazione della Corte circa un presunto errore di traduzione nella versione italiana delle sentenze CGUE non fosse condivisibile, in quanto il legislatore Ue, quando ha voluto riferirsi al concetto di "autorità giudiziaria", ha usato il termine inglese "judicial authority" o quello francese "autorité judiciaire" e non quelli di *Court* e *jurisdiction* [128]; che gli stessi termini *Court* e *jurisdiction* sono comunque riferibili, nei rispettivi ordinamenti, ad organi posti in posizione di terzietà rispetto alle parti e non ricomprendono il ruolo della magistratura inquirente[129]. La Suprema Corte avrebbe in realtà inteso preservare a tutti costi la possibilità delle autorità di *law enforcement* di avvalersi di un meccanismo essenziale per la lotta alla criminalità come *la data retention*[130]. Dunque, un "braccio di ferro" -verificatosi anche in altri Stati membri - tra le autorità statali, desiderose di sfruttare le potenzialità di indagine della conservazione dei dati di traffico, e la resistenza opposta dalla Corte di giustizia e dalla Corte Europea dei Diritti dell'Uomo, tesa a ricondurre l'ambito di una simile ingerenza nel diritto alla tutela dei dati personali entro i parametri di un

119. In banca dati *Dejure*.

120. In banca dati *Dejure*.

121. In banca dati *Dejure*.

122. Posizione analoga a quella dei giudici di legittimità era stata assunta da una delle rare decisioni di merito che si era occupata della questione. Il Tribunale di Padova, con l'ordinanza del 15.3.2017 (in *Diritto penale contemporaneo)*, pronunciata dopo la sentenza della Corte di giustizia *Digital Rights Ireland Ltd*, aveva ritenuto che la sentenza della Corte di giustizia non potesse avere effetto sull'art. 132 cod. privacy e che nel caso di specie, in ragione della gravità delle fattispecie per cui erano stati acquisiti i dati del traffico telefonico, il principio di proporzionalità fosse stato pienamente rispettato. Per una nota di commento: Flor R., *Data retention ed art. 132 cod. Privacy: vexata questio?*, in *Diritto penale contemporaneo* (*archiviodpc.dirittopenaleuomo.org*), 2017.

123. Luparia L., *Data retention e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, in *Diritto di Internet,* 4, 2019, pp.753-764.

124. Torre F., cit., p. 540 e p.548.

125. Malacarne A.-Tessitore G., cit., p.21.

126. Greco C., cit., pp. 252-253.

127. Luparia L., 2019, cit., p.762.

128. Luparia L., 2019, cit., p.762.

129. Neroni Rezende I., *Dati esterni alle comunicazioni e processo penale: questioni ancora aperte in tema di data retention,* in *Sistema* Penale, 5, 2020, p.192; Torre F., cit., p.548.

130. Luparia L., 2019, cit., p.764. In questo senso anche Rinaldini F., op. cit., p.7.

giudizio di proporzionalità[131].

Questo approccio della giurisprudenza nostrana pare essersi sostanzialmente protratto oltre la pronuncia della sentenza H.K. del 2.3.2021. In merito a quest'ultima, il Tribunale di Milano, con ordinanza del 22.4.2021[132] , aveva considerato che, attesi i connotati che differenziano il Pubblico Ministero estone da quello italiano (come si ricorderà, la sentenza H.K. è stata pronunciata in un caso riguardante l'Estonia) ed in ragione delle costanti pronunce della Corte di Cassazione, non fosse possibile ravvisare alcun profilo di censura dell'art. 132 D.lgs. n.196 del 30.6.2003 per contrarietà all'articolo 15, paragrafo 1, della direttiva 2002/58/CE e che, in ogni caso, la sentenza della Corte di giustizia non avrebbe potuto essere applicata retroattivamente. Il Tribunale aveva pertanto acquisito i tabulati richiesti dal Pubblico Ministero. Con provvedimento del 29.4.2021 il Giudice per le indagini preliminari presso il Tribunale di Roma, premesso che la sentenza H.K. non poteva avere effetti immediati e diretti nel nostro ordinamento giuridico a causa della propria indeterminatezza circa i casi nei quali i dati del traffico possono essere acquisiti, aveva ritenuto che l'art.132 D.lgs. n.196 del 30.6.2003 dovesse continuare a trovare applicazione[133]. Anche un'ordinanza dell'Ufficio del Giudice per le indagini preliminari presso il Tribunale di Tivoli del 9.6.2021 ed un'ordinanza della Corte di Assise di Napoli, Sezione prima penale, del 16.6.2021 avevano negato la diretta applicabilità della sentenza H.K nell'ordinamento italiano[134]. Alle stesse conclusioni era pervenuta la Corte di Cassazione[135] secondo la quale la sentenza H.K. non poteva avere efficacia diretta, in quanto del tutto generica nell'individuazione dei casi di legittima acquisizione dei dati di traffico telefonico e telematico. Dovendosi pertanto, secondo il giudice di legittimità, demandare al legislatore nazionale il compito di trasfondere in una legge dello Stato i principi delineati dalla Corte di Giustizia.[136].

Anche questi arresti "post sentenza H.K." hanno suscitato perplessità. Pur ammettendo la non autosufficienza delle argomentazioni della sentenza H.K e la non applicabilità in via diretta della Dir. 2002/58/CE (la direttiva *E-privacy* che, per la propria natura di direttiva, non contiene disposizioni puntuali), sarebbe stato possibile sollevare questione di incostituzionalità del previgente 132 D.lgs. n.196 del 30.6.2003 per violazione dell'art. 117, primo comma, della Costituzione (che impone al legislatore il rispetto dei vincoli derivanti dall'ordinamento comunitario e dagli obblighi internazionali), od operare un rinvio pregiudiziale ex art. 267 TFUE, interpellando la Corte di giustizia circa la conformità della normativa italiana al diritto eurounitario[137]. Un rinvio pregiudiziale al giudice europeo in tal senso era stato invece effettuato unicamente dal Tribunale di Rieti con ordinanza del 4.5.2021[138].

131. Ponti B., *Il rapporto tra cybersicurezza e tutela dei dati personali: sinergie, bilanciamenti e parallelismi*, in *Rivista Italiana di Informatica e Diritto*, 2, 2024, p.151.

132. Tribunale Milano, VII sezione penale, ordinanza del 22.4.2021. Per il testo dell'ordinanza ed un commento: Tondi V. *La disciplina italiana in materia di data retention a seguito della Corte di Giustizia UE: Il Tribunale di Milano nega il contrasto con il diritto sovranazionale*, in *Sistema Penale*, 2021.

133. Si veda: Malacarne A., *Ancora sulle ricadute interne della sentenza della Corte di giustizia in materia di acquisizione di tabulati telefonici: il G.I.P. di Roma dichiara il "non luogo a provvedere" sulla richiesta del P.M*, in *Sistema Penale*, 2021.

134. Per una nota di commento ed il testo delle citate ordinanze: Stampanoni Bassi G. (a cura di), *Acquisizione dei dati telefonici: il Tribunale di Tivoli si pronuncia sull'efficacia della sentenza CGUE del 2 marzo 2021 (C 746/18)*, in *Giurisprudenza Penale Web*, 2021; Id. (a cura di), *Acquisizione dei tabulati telefonici: anche la Corte di Assise di Napoli esclude un'applicazione diretta della sentenza CGUE del 2 marzo 2021 (C 746/18)*, in *Giurisprudenza Penale Web*, 2021.

135. Corte di Cassazione, Seconda Sezione Penale, sentenza n. 33116 del 7.9.2021. Per una nota di commento ed il testo: Stampanoni Bassi G. (a cura di), *Acquisizione dei tabulati telefonici: anche la Corte di Cassazione esclude una applicazione diretta della sentenza CGUE del 2 marzo 2021 (C 746/18)*, in *Giurisprudenza Penale Web*, 2021.

136. Solo in apparente discontinuità con questo orientamento si era posto il decreto dell'Ufficio del Giudice per le indagini preliminari presso il Tribunale di Roma del 25.4.2021 (in *Sistema Penale,*2021). Da una parte, il decreto aveva ravvisato un sopravvenuto contrasto tra l'art. l'art.132, comma 3, D.lgs. n.196 del 30.6.2003 e la normativa dell'Unione Europea, come interpretata dalla Corte di giustizia, nella parte in cui attribuiva al Pubblico Ministero la competenza ad acquisire i dati. Il provvedimento aveva altresì sostenuto la possibilità di fare applicazione diretta nel nostro ordinamento giuridico della sentenza H.K., nonostante la mancanza di una indicazione dei "gravi reati" in presenza dei quali poter disporre l'acquisizione dei dati di traffico. Dall'altra, lo stesso decreto aveva ritenuto che, per ovviare alla mancata indicazione dei "gravi reati", si sarebbe potuto attingere al catalogo di cui alla disciplina delle intercettazioni telefoniche e telematiche ed aveva pertanto, all'esito di questo percorso argomentativo, autorizzato l'acquisizione dei dati medesimi.

137. In questo senso Torre F., op. cit., p.550; La Rocca E.N., cit., p.4; Rafaraci T., cit., p. 854; Filippi L., *Il decreto legge sui tabulati, in Penale Diritto e Procedura,* 3, 2021.

138. Nell'ordinanza (in *Giurisprudenza penale web,* 2021) il Tribunale aveva chiesto alla CGUE di verificare, alla luce della sentenza

Solo grazie alla riforma attuata mediante il D.L. n. 132 del 30.09.2021 (e la sua conversione con modificazioni ad opera della L. n. 178 del 23.11.2021) la disciplina italiana della *data retention* risulta maggiormente in armonia con le indicazioni della giurisprudenza europea e con l'esigenza di garantire i diritti fondamentali. Innestando nell'art. 132 D.lgs. n.196 del 30.6.2003 una serie di presupposti applicativi (la necessità che si proceda per determinati reati, la sussistenza di sufficienti indizi di tali reati, il requisito della rilevanza dell'acquisizione dei "dati esterni" per l'accertamento dei fatti) il legislatore ha dato un contenuto precettivo al profilo motivazionale del provvedimento, che nella disposizione previgente era solo implicito[139]. Inoltre, la previsione, con la novella del 2021, di un vaglio giurisdizionale (è richiesto il decreto motivato di autorizzazione del giudice) integra un più elevato standard garantistico che dà piena attuazione alla riserva di giurisdizione dell'art.15 Cost.[140] La nuova disciplina comporta peraltro che il giudice in motivazione dia conto della sussistenza di risultanze investigative idonee a raffigurare un apprezzabile *fumus* delle condotte per cui di procede[141]. Sarebbe così evitato il concreto pericolo di legittimare indagini *ad explorandum*, in quanto il decreto autorizzativo del giudice, nel rispetto del principio di proporzionalità, dovrebbe prevedere un accesso limitato ai soli dati che presentano un nesso di pertinenzialità con il reato da accertare[142]. Per di più, la legge di conversione ha introdotto, per i tabulati acquisiti in procedimenti penali in data precedente all'entrata in vigore della riforma, un regime transitorio, a tenore del quale essi sono utilizzabili a carico dell'imputato solo se relativi al catalogo dei reati di cui al "nuovo" comma 3 dell'art. 132 Cod. priv. e solo "unitamente ad altri elementi di prova". Con tale espressione intendendosi che il giudice dovrà seguire lo stesso percorso valutativo previsto per la chiamata in correità, esigendosi dunque i c.d. riscontri estrinseci[143]. In definitiva, il potere di acquisizione dei dati esterni (e di limitazione dei diritti coinvolti) risulta maggiormente circoscritto, con un aggravamento dell'onere motivazionale dell'autorità che procede.

La recente riforma, pur potendo essere salutata con favore, non è priva di criticità[144]. Vi sono due aspetti problematici della disciplina italiana ad oggi in vigore sui quali sembra opportuno soffermarsi: quello del più esteso periodo di conservazione dei dati di traffico ed ubicazione per alcuni gravi reati e quello della "lista" dei reati che legittimano la procedura di acquisizione dei metadati.

Il primo profilo da dibattere attiene, come detto, al periodo di conservazione dei dati esterni del traffico. Occorre premettere che la riforma del 2021 è intervenuta sulla procedura di acquisizione dei tabulati, ma non ha inciso sui termini -decorrenti dalla data della comunicazione elettronica- entro i quali il fornitore del servizio deve conservarli, che sono tuttora quelli di cui ai commi 1, 1 bis e 5 bis dell'art. 132 Cod. priv. Precisamente, come noto, i commi 1 ed 1 bis tracciano un regime ordinario, legato alla generica "finalità di accertamento e repressione dei reati", a tenore del quale il periodo di conservazione è di ventiquattro mesi per i dati relativi al traffico telefonico, dodici mesi per i dati relativi al traffico telematico e di trenta giorni per i dati relativi

---

H.K.: se il Pubblico Ministero italiano potesse acquisire i tabulati; in caso negativo, se i principi di "H.K." potessero essere applicati retroattivamente; infine, se il Pubblico Ministero potesse acquisire in via d'urgenza i tabulati. Nelle more della decisione della Corte di Giustizia, è intervenuta la riforma qui in commento.

139. *Corte Suprema di Cassazione. Relazione su novità normativa. 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)*, n.55 del 2021, p. 21. E' stato tuttavia osservato che, per evitare l'adozione di "formule di stile", sarebbe stato opportuno prevedere altresì un onere di motivazione rafforzata sui presupposti dell'acquisizione dei dati. Filippi L., *Tabulati telefonici e telematici e rispetto della vita privata*, in *Diritto di difesa,* 2022*,* p.14.

140. Ibidem, p.22.

141. Ibidem, p.25.

142. Murro O., 2022, cit., p.2448.

143. *Corte Suprema di Cassazione*. *Relazione su novità normativa*. *Conversione in legge, con modificazioni, del decreto-legge 30 settembre 2021, n.132, recante misure urgenti in materia di giustizia (legge 23 novembre 2021, n.178)*, n. 67 del 2021, In *https://www.giurisprudenzapenale.com*, p.8. E'stato tuttavia obiettato che la formula "solo unitamente ad altri elementi di prova" non aggiunge o toglie nulla agli ordinari criteri probatori, atteso che i tabulati di per sé non dicono nulla sui fatti oggetto del giudizio. Pestelli G., cit., p.5. In ogni caso, la Corte di Cassazione, con la sentenza n. 29268 della Sezione quinta penale depositata il 18.7.2024 (in *https://www.cortedicassazione.it.*), ha aderito all'orientamento giurisprudenziale per il quale la regola secondo cui i tabulati possono essere valutati solo unitamente ad altri elementi di prova è sottratta, in quanto regola legale di valutazione della prova, al principio processuale del "tempus regit actum" ed è pertanto applicabile anche ai tabulati acquisiti in procedimenti penali prima dell'entrata in vigore D.L. n.132 del 30.9.2021.

144. Per un quadro degli aspetti critici, si vedano, tra gli altri: Tavassi L., cit., pp.11-12; Tartara V., cit., p. 194.

alle chiamate senza risposta. Questi termini "ordinari", soffrono però una deroga ad opera del comma 5 bis, che, mediante il richiamo all'art. 24 della legge 20.11.2017, n. 167 (la legge europea per il 2017), prevede un termine di conservazione dei dati (relativi al traffico telefonico e telematico e alle chiamate senza risposta) di settantadue mesi, per la finalità dell'accertamento e della repressione di alcuni gravi reati: quelli di cui agli articoli 51, comma 3 *-quater*, e 407, comma 2, lettera *a)*, C.P.P. (cioè i delitti consumati o tentati con finalità di terrorismo e quelli, nominativamente indicati dall'art. 407 c.p.p., per i quali il termine massimo di durata delle indagini preliminari è innalzato a due anni).

Contro il termine di settantadue mesi si sono indirizzati gli strali della dottrina, e non soltanto di essa, che vi ha in sintesi ravvisato un grave sbilanciamento nel rapporto tra il perseguimento della sicurezza pubblica ed il rispetto dei diritti fondamentali. La durata di sei anni della conservazione dei dati è stata ritenuta irragionevole[145] e costituente un lasso temporale eccessivamente esteso, non tollerabile in uno stato democratico[146]. Si è inoltre considerato che, secondo la giurisprudenza della Corte di Giustizia, la distinzione tra criminalità grave e criminalità comune non dovrebbe condurre a differenziare la durata del periodo di conservazione, ma soltanto a differenziare i tipi di dati conservabili (traffico, ubicazione o identità civile)[147]. Infatti, nelle argomentazioni della Corte rileverebbe soltanto il grado di ingerenza nei diritti fondamentali, ovvero la possibilità che dai dati raccolti possano trarsi conclusioni precise in merito alla vita privata dell'utente.[148]

Il termine di sei anni pone anche un altro correlato tema: il fornitore di servizi, non potendo prevedere le richieste che gli perverranno in futuro, custodirà in ogni caso per settantadue mesi tutti i dati di traffico[149]. Con la conseguenza che l'amplissimo termine in questione, formalmente riferito in via di deroga solo ad alcuni gravi reati, finisce inevitabilmente per applicarsi alla conservazione di ogni metadato. I termini ordinari soccombono a favore del termine speciale, con un'inversione del rapporto tra regola ed eccezione che solleva dubbi di costituzionalità e di tensione della disposizione con il diritto europeo[150].

Quanto appena detto può essere valutato seguendo anche un'altra prospettiva. A questa disciplina potrebbero essere infatti mosse le obiezioni concernenti l'(in)opportunità di delegare il governo della rete e dei dati agli Internet Service Providers. In generale, la "delega" agli ISP presenta criticità relative alla delicatezza di affidare loro attività che attengono al diritto e alla libertà di disporre dei propri dati privati[151]. Più in particolare, può essere qui ricordata l'obiezione concernente il rischio che il provider, una volta gravato di obblighi in tal senso, eserciti una sorta di ipercontrollo, ovvero un controllo molto severo sulle informazioni e sui contenuti (ad esempio, mediante *over-filtering* o *over-blocking*), vestendo i panni di un censore per evitare di incorrere in contestazioni e per sottrarsi alla costante minaccia di azioni legali[152]. Un ipercontrollo si concretizza, come visto, proprio rispetto agli obblighi in materia di *data retention*, per rispettare i quali il fornitore è tenuto di fatto a "congelare" sino a sei anni ogni dato di traffico, generato con qualsiasi mezzo di comunicazione elettronica, da chiunque ed a prescindere dall'esistenza di un nesso con fattispecie di reato o dall'instaurazione di un procedimento penale. Questo aspetto è stato messo in rilievo anche dal Garante per la protezione dei dati personali, che sull'istituto si era espresso, poco dopo la pronuncia della sentenza H.K., con la *"Segnalazione sulla disciplina della conservazione, a fini di giustizia, dei dati di traffico telefonico e telematico" del* 22.7.2021[153]. In merito al periodo di conservazione per settantadue mesi, il Garante ne ha sottolineato la carenza di proporzionalità, non ritenendo sufficiente che l'acquisibilità dei dati raccolti oltre il termine ordinario sia limitata

145. Filippi L., *Tabulati telefonici e telematici e rispetto della vita privata*, 2022, cit., p.13

146. Sambuco G., cit., p.14.

147. Greco C., cit., p.253.

148. Ibidem, p. 253.

149. Torre F., cit., p.543.

150. Flor R.-Marcolini S., op. cit., p.106.

151. Luparia L., *Il sistema penale ai tempi dell'Internet. La figura del provider tra diritto e processo*, in Luparia, L. (a cura di), *Internet provider e giustizia penale*, Giuffré, 2012, p.8.

152. Cfr. Ziccardi G., *L'odio online. Violenza verbale e ossessioni in rete*, Raffaele Cortina Editore, 2016, p. 243; Colomba V., *I diritti nel cyberspazio. Architetture e modelli di regolazione.* Diabasis, 2016., p.66; Caletti, G.M., *Habeas corpus digitale. Lo statuto penale dell'immagine corporea tra privatezza e riservatezza*, Giappichelli, 2024, p.39.

153. Doc-Web 9685978, sul sito *https://www.garanteprivacy.it/.*

a una categoria di reati particolarmente gravi, in quanto *"proprio la natura retrospettiva di questo strumento investigativo implica la conservazione generalizzata dei dati di traffico per sei anni, salvo poi limitarne l'utilizzabilità processuale ai soli casi normativamente considerati"*. Si realizzerebbe dunque una massiva raccolta di dati la quale - per la loro utilizzabilità limitata- non solo non è probabilmente coerente con il principio di proporzionalità tra esigenze investigative e privacy[154], ma comporta la creazione di una "banca dati" -cui attingere in caso di utilità e necessità investigativa- illegittima alla luce della giurisprudenza della Corte di Giustizia[155]. In questo senso, può rammentarsi che la Corte di Giustizia medesima aveva invalidato la già più volte citata Direttiva "Frattini" (2006/24/CE del 15.3.2006) che imponeva un termine di conservazione dei dati inferiore a quello di cui qui si discute.[156] Si tratta peraltro di una disciplina, quella italiana, in evidente controtendenza rispetto ai principi che hanno ispirato il *GDPR* (Regolamento UE n. 2016/679) ed a quelli delle normative di altri Stati membri dell'Ue, maggiormente rispettose del diritto alla privacy in materia di termini di conservazione dei metadati[157].

Pertanto, ad avviso di chi scrive può considerarsi censurabile che il legislatore non sia intervenuto sull'istituto della conservazione di settantadue mesi, per rimodularlo e modificarne i presupposti, né con il D.lgs. n. 101 del 10.8.2018 (di adeguamento della normativa nazionale alle disposizioni del Regolamento europeo sulla protezione dei dati personali), né con il D.lgs. n. 51 del 18.5.2018 (di attuazione della direttiva UE sul trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali), né nel 2021 con la riforma dell'art. 132 del Codice della privacy. Vi è chi ritiene che l'art. 24 della legge 20.11.2017, n. 167, che come visto prevede il termine in questione, dovrebbe essere *tout court* abrogato[158].

Qualche considerazione può essere svolta, infine, anche rispetto ad un altro punto della riforma. La sentenza H.K (§ 33) ha affermato che soltanto la lotta contro le "forme gravi di criminalità" e la prevenzione di "gravi minacce alla sicurezza pubblica" sono idonee a giustificare ingerenze gravi nei diritti fondamentali al rispetto della vita privata e familiare e alla protezione dei dati personali, come quelle che comporta la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione. Per conformare la legislazione italiana alla sentenza, la riforma del 2021 ha previsto che la procedura di acquisizione dei tabulati possa essere esperita solo in relazione a delitti per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni ed ai reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi (nuovo comma 3 dell'art. 132 D.lgs. n.196 del 30.6.2003). Categorie di reati utilizzati anche per regolare l'applicazione della disciplina transitoria (art.1, comma 1-bis, L. 23.11. 2021 n.178).

Ciò premesso, ci si può domandare se tale novero di reati possa considerarsi rispettoso del principio, statuito dalla Corte di Giustizia, secondo cui i diritti fondamentali possono subire una compressione solo in presenza di atti illeciti gravi.

Secondo una prima opinione, il perimetro dei reati presupposto della procedura di acquisizione dei dati supera gli ambiti delineati dalla Corte di Giustizia[159] ed il legislatore italiano avrebbe fornito un'interpretazione "generosa" delle forme gravi di criminalità e della prevenzione di gravi minacce alla sicurezza pubblica, mentre sarebbe stato preferibile un innalzamento della soglia di punibilità a cinque anni ed una più attenta perime-

154. Spangher G., *Conservazione dei dati e diritto alla riservatezza. La Corte di Giustizia interviene sulla data retention. I riflessi sulla disciplina interna*, in *Giustizia insieme*, 2021, p.4.

155. Di Stefano G., cit., p.363.

156. Cfr. Cardone A., *Il sistema del Data Retention come strumento* investigativo**,** in *Giurisprudenza penale Web*, 2021, p.4.

157. Giangreco M., cit., p.1675. La conservazione di dati personali per un così lungo periodo pone inoltre la questione della loro sicurezza di fronte al rischio di *data breach*. Ibidem, p.1675. I rischi relativi alla *cybersecurity* nella conservazione dei dati di traffico e di ubicazione sono stati rilevati dalla Corte di Giustizia UE, la quale ha considerato che *"tenuto conto della quantità rilevante di dati relativi al traffico ed all'ubicazione conservati continuativamente mediante una misura di conservazione generalizzata ed indiscriminata, nonché del carattere delicato delle informazioni che tali dati possono fornire, la conservazione di questi dati da parte dei fornitori di servizi di comunicazione elettronica comporta di per sé rischi di abuso e di accesso illecito"*. Corte di Giustizia, Grande Sezione, sentenza del 20.9.2022 (cause riunite C-793/19 e C-794/2019) § 62 e giurisprudenza ivi citata.

158. Greco C., cit., p.254.

159. Murro O., 2022. cit., p. 2446.

trazione dei fatti costituenti reato meritevoli di tutela[160]. Le fattispecie dell'elenco non sarebbero state selezionate in funzione dei bene giuridici protetti, con la conseguenza che non necessariamente ledono o mettono in pericolo l'ordine pubblico[161].

Altri ha ritenuto, al contrario, che i limiti edittali siano troppo bassi, e che ciò produca la conseguenza di pregiudicare anche le attività acquisitive compiute in merito a reati "odiosi", tra cui la sostituzione di persona mediante creazione di un falso account o mediante utilizzo dell'identità altrui per l'acquisto di beni o l'attivazione di servizi, le diffamazioni non aggravate, (ad esempio quelle compiute mediante l'invio di mail o messaggi a più destinatari senza pubblicazione online), nonchè la diffusione di programmi malevoli[162].

Pare a chi scrive preferibile la tesi secondo la quale l'attuale previsione dei reati per i quali è ammessa la procedura di acquisizione dei dati di traffico e di ubicazione sia ad oggi eccessivamente ampia. Da una parte, è vero che la Corte di Giustizia non si sia spinta a definire cosa intenda per forme gravi di criminalità e gravi minacce alla sicurezza pubblica. Dall'altra, la stessa Corte ha in alcune occasioni esemplificato le fattispecie ed i beni giuridici da proteggere relativi a queste categorie, facendo riferimento alla lotta contro il terrorismo internazionale e contro la criminalità grave al fine di garantire la sicurezza pubblica[163]; alla criminalità organizzata e al terrorismo[164]; alla salvaguardia della sicurezza nazionale e, in particolare, al terrorismo[165]; alle attività di terrorismo[166]. Già queste indicazioni, pur fornite dalla giurisprudenza eurounitaria senza pretese di esaustività, non appaiono in armonia con l'inclusione di reati puniti con la reclusione non inferiore nel massimo a tre anni e dei reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, seppure solo quando gravi.

Tenuto conto degli approdi della giurisprudenza della Corte di Giustizia europea sin qui richiamata, la previsione di un tetto di tre anni di reclusione nel massimo presenta una capacità selettiva ridotta. Sul punto, sembra opportuno osservare che la L. 28.6.2024 n. 90. ("Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici") ha inasprito in misura molto rilevante le pene per le principali figure di *cybercrimes,* intervenendo sulla pena delle fattispecie base, oppure su quella delle fattispecie aggravate o introducendo nuove ipotesi di circostanze aggravanti ad effetto speciale. Perciò il limite dell'art. 132 D.lgs. n.196 del 30.6.2003 di tre anni nel massimo potrebbe essere innalzato, senza che ciò precluda necessariamente l'acquisizione dei metadati concernenti la maggior parte dei reati "informatici" previsti dal Codice penale.

Alcune ulteriori riflessioni merita l'inclusione, tra i reati presupposto, della minaccia e della molestia o disturbo alle persone col mezzo del telefono quando la minaccia, la molestia e il disturbo siano gravi. Innanzi tutto, minaccia, molestia e disturbo gravi sono reati la cui punibilità sembra possa difficilmente trovare fondamento in una esigenza di contrasto a "forme gravi di criminalità" o di "prevenzione di gravi minacce alla sicurezza pubblica", secondo quanto richiesto dalla Corte di Giustizia. Inoltre, mentre il concetto di "minaccia grave" è presente dal codice penale ed ha solidi riferimenti giurisprudenziali, i concetti di molestia e disturbo "gravi" appaiono del tutto nuovi e si presterebbero ad interpretazioni discrezionali ed incerte, rendendo impossibile la prevedibilità delle decisioni[167]. La "gravità" delle minacce, delle molestie e del disturbo alle persone dovrebbe infatti essere oggetto di una valutazione in concreto da parte del giudice. Tuttavia, la giurisprudenza del giudice di Lussemburgo imporrebbe l'applicazione del canone della proporzionalità in astratto, non rimesso

160. Giangreco M., cit., p.1681.

161. Tavassi L., cit., p.11.

162. Pestelli G., cit., pp.5-6.

163. Corte di Giustizia, Grande Sezione, sentenza dell'8.4.2014 *(*cause riunite C-293/12 e C-594/12 C-140/20, *Digital Rights Ireland Ltd*), cit., § 42.

164. Corte di Giustizia, Grande Sezione, sentenza del 21.12.2016 *(*cause riunite C-203/15 e C 698/15, *Tele2 Sverige*), cit., § 103.

165. Corte di Giustizia, Grande Sezione, sentenza del 6.10.2020 *(*cause riunite C-511/18, C-512/18 e C-520/18 *Le Quadrature du Net* ed altri), cit., § 135.

166. Corte di Giustizia, Grande Sezione, sentenza del 5.4.2022 *(*causa C-140/20, *G.D. contro Commissioner of An Garda Siochána* ed altri), cit., § 61 e giurisprudenza ivi menzionata.

167. Si veda: *Corte Suprema di Cassazione. Relazione su novità normativa. Misure urgenti in tema di acquisizione dei dati relativi al traffico telefonico e telematico a fini di indagine penale*, cit., p.24.

alla discrezionalità caso per caso[168]. In tal senso può essere interpretata l'affermazione secondo cui "*Per soddisfare il requisito di proporzionalità, una normativa nazionale deve prevedere norme chiare e precise che disciplinino la portata e l'applicazione della misura considerata e fissino un minimo di requisiti, di modo che le persone i cui dati personali siano oggetto di attenzione dispongano di garanzie sufficienti che consentano di proteggere efficacemente tali dati contro i rischi di abuso"*[169]. Anche la sentenza H.K. non sembra ammettere un vaglio di proporzionalità in concreto e valutazioni discrezionali dell'utilizzatore dei dati emersi dai controlli occulti[170]. Si potrebbe in aggiunta osservare che se anche si escludessero le minacce e le molestie dalla procedura di acquisizione dei tabulati, le condotte previste da tali fattispecie potrebbero restare comunque assoggettabili a detta procedura ogni volta in cui integrino l'elemento materiale di altre più gravi fattispecie come, ad esempio, l'estorsione, la violenza privata, gli atti persecutori.

Sulla questione dei "reati-presupposto", e proprio sul nostro Codice della privacy, è intervenuta recentemente la Corte di giustizia, la quale, con la sentenza resa il 30.4.2024[171], ha ritenuto che il vigente art. 132 D.lgs. n.196 del 30.6.2003 non sia contrastante con il diritto europeo. La Corte si è pronunciata a seguito di domanda di pronuncia pregiudiziale proposta dal Giudice delle indagini preliminari presso il Tribunale di Bolzano, il quale aveva formulato dubbi circa la compatibilità dell'articolo 132, comma 3, Codice della privacy con l'articolo 15, paragrafo 1, della direttiva 2002/58/CE. In particolare, il giudice del rinvio aveva osservato che la soglia dei tre anni di pena detentiva nel massimo è tale che i tabulati telefonici potrebbero essere comunicati alle autorità pubbliche per perseguire reati che destano solo scarso allarme sociale e che sono puniti solo a querela di parte. La Corte di Lussemburgo ha invece concluso che non è in contrasto con il diritto dell'UE una disposizione nazionale che imponga al giudice di autorizzare l'accesso a un insieme di dati relativi al traffico o di dati relativi all'ubicazione, qualora detto accesso sia richiesto ai fini dell'accertamento di reati puniti dal diritto nazionale con la pena della reclusione non inferiore nel massimo a tre anni. Purché, ha proseguito la Corte, sussistano sufficienti indizi di tali reati, i dati siano rilevanti per l'accertamento dei fatti e a condizione che il giudice nazionale abbia la possibilità di negare l'accesso se questo è richiesto nell'ambito di un'indagine su un reato manifestamente non grave, alla luce delle condizioni sociali esistenti nello Stato membro interessato.

Si potrebbe osservare, in primo luogo, come la Corte, rimettendo in ultima analisi la valutazione della gravità al giudice (in base alle "condizioni sociali dello Stato membro"), abbia in sostanza scelto un concetto di proporzionalità in concreto che si pone in discontinuità con la precedente giurisprudenza della stessa Corte di giustizia e che può altresì essere foriero di incertezze. Esso potrebbe infatti rendere più arduo l'obiettivo di un'uniforme interpretazione ed applicazione, nell'ambito eurounionale, di quei presidi del principio di proporzionalità costituiti dai concetti di "lotta contro le forme gravi di criminalità" e di "prevenzione di gravi minacce alla sicurezza pubblica". In secondo luogo, la pronuncia ha legittimato un limite edittale, come quello italiano, che rende ammissibile la procedura di acquisizione dei metadati per la gran parte dei delitti previsti dall'ordinamento giuridico, appagandosi la Corte della possibilità che il giudice possa negare l'autorizzazione in presenza di un reato "manifestamente non grave"[172]. Il parametro di garanzia risulterebbe così abbassato. Peraltro, vi sono ragioni per ritenere che il concetto di gravità -al quale fa riferimento la Corte nella sentenza in questione- non riguardi il disvalore del fatto commesso, in quanto il riferimento alle "condizioni sociali" pare invece evocare considerazioni concernenti il disvalore e l'allarme sociale che connotano una certa tipologia di illeciti nel contesto di riferimento, col rischio di provocare uno sconfinamento del giudice sul terreno

168. Torre F., cit., p 549.

169. Corte di Giustizia, Grande Sezione, sentenza del 20.9.2022 (cause riunite C-793/19 e C-794/19, *SpaceNet AG e Telekom Deutschland*), cit., § 69 e giurisprudenza ivi citata.

170. La Rocca E. N., cit., p.2.

171. Corte di Giustizia, Grande sezione, sentenza del 30.4.2024 (causa C-178/22). In *https://curia.europa.eu/juris.*

172. Vi è chi ha giudicato favorevolmente la possibilità, riconosciuta al giudice nazionale dalla Corte di Giustizia, di valutare la non manifesta gravità dei reati. In questo modo sarebbe stata temperata la rigida regola secondo cui la valutazione di gravità è effettuata una volta per tutte dal legislatore e la presunzione assoluta di gravità, basata sui limiti edittali stabiliti, è stata trasformata in una presunzione relativa. Todaro G., cit., p.2036. Anche secondo Albanese (Albanese, D., *Dalla Corte di giustizia dell'Unione Europea un'altra svolta garantista in materia di acquisizione dei tabulati telefonici*. In *Sistema penale*, 5, 2024, p. 98) la sentenza rappresenta un'ulteriore svolta garantista, in quanto comporta che la disposizione italiana, per potersi armonizzare con la normativa sovranazionale, debba essere integrata da un test di proporzionalità.

della politica criminale[173]. Eventuali prossime pronunce consentiranno forse meglio di comprendere se la Corte di giustizia abbia correttamente interpretato sé stessa, od abbia invece compiuto un passo indietro nella protezione dei diritti fondamentali in materia di sorveglianza digitale[174].

6 Bibliografia

Albanese D., *Dalla Corte di giustizia dell'Unione Europea un'altra svolta garantista in materia di acquisizione dei tabulati telefonici*, in *Sistema penale*, 5, 2024, p. 98.

Alexy R., *Teoria dei diritti fondamentali*, Il Mulino, 2012.

Baccari G.M., *Il trattamento (anche elettronico) di dati personali per finalità di accertamento di reati*, in Cadoppi A.-Canestrari S.-Manna A.- Papa M. (Dir.) *Cybercrime*, seconda edizione, Utet Giuridica, 2023, pp. 1876, 1871-1881, 1869.

Bongiovanni G., *Diritti inviolabili e libertà*, in Barbera A. (a cura di), *Le basi filosofiche del costituzionalismo*, Laterza, 2019, p.86.

Caletti G.M., *Habeas corpus digitale. Lo statuto penale dell'immagine corporea tra privatezza e riservatezza*, Giappichelli, 2024, p. 39.

Cardone A., *Il sistema del Data Retention come strumento* investigativo**,** in *Giurisprudenza penale Web*, 2021, p. 4.

Caretti P.- Tarli Barbieri G., *I Diritti Fondamentali. Libertà e Diritti sociali*, Giappichelli, 2022, pp. XXXI-XXXII, 39, 14.

Càrpino M., *Il trattamento dei dati personali per finalità di prevenzione, indagine, accertamento e perseguimento di reati*, Giappichelli, 2024.

Colomba V., *I diritti nel cyberspazio. Architetture e modelli di regolazione,* Diabasis, 2016.

Conti C., *Sicurezza e riservatezza*, in *Diritto penale e processo*, 11, 2019, pp.1574-1575, 1578.

Conti C., *La corsa tecnologica tra Costituzione, codice di rito e norme sulla privacy: uno sguardo d'insieme*, in *Diritto penale e processo*, 6, 2021, p.716.

Conti C., *La prova informatica e il mancato rispetto delle best practices*, in Cadoppi A.-Canestrari S.-Manna A.- Papa M. (diretto da), seconda edizione, Utet Giuridica, 2023, pp.1542-1543.

Corte Suprema di Cassazione. *Relazione su novità normativa. 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)*, n.55 del 2021, in *https://www.cortedicassazione.it*.

Corte Suprema di Cassazione. *Relazione su novità normativa. Conversione in legge, con modificazioni, del decreto-legge 30 settembre 2021, n.132, recante misure urgenti in materia di giustizia (legge 23 novembre 2021, n.178)*, n. 67 del 2021, in *https://www.giurisprudenzapenale.com*, p.8.

Croci L., *La Corte Penale Internazionale e le prove digitali. Gestione, sfide e innovazioni nell'era digitale*, in questa Rivista, 18,1, 2025, pp. 4-5.

Della Torre J.-Malacarne A., *L'utilizzo dei file di log per scopi di contrasto alla criminalità: nodi problematici e possibili soluzioni*, in *Archivio penale Web*, 2, 2022, 1-22.

173. Parodi, L. 2025., La "gravità dell'ingerenza" nel prisma della proporzionalità: nuovi equilibri in tema di data retention. In *Sistema penale (https://www.sistemapenale.it),* p.18.

174. Una nuova pronuncia della Corte di Giustizia sulla disciplina italiana potrebbe prospettarsi a breve. Infatti, il Giudice per le indagini preliminari presso il Tribunale di Catania ha emesso, il 26.6.2025, un'ordinanza di rinvio pregiudiziale alla Corte di Giustizia (in *Sistema penale,* 2025), interrogando la Corte sulla necessità o meno di rispettare le disposizioni previste in tema di *data retention* anche in caso di accesso delle autorità pubbliche ai *file di log*, al solo fine di identificare l'autore di un reato.

Demartis F. *La nuova disciplina sui tabulati: un completo adeguamento agli standard europei?*, in *Diritto penale e processo*, 3, 2022, p. 307.

Di Stefano G., *La Corte di Giustizia conferma la regola del divieto, con eccezioni, di conservazione dei dati di traffico telefonico e telematico ai fini di lotta alla criminalità grave: la fine della prova a mezzo di tabulati?*, in *Cassazione penale*, 1, 2023, pp. 354-367.

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

Id., *Tabulati telefonici e telematici e rispetto della vita privata*, in *Diritto di difesa,* 2022, pp. 5-6, 13, 14.

Id., *Riservatezza e data retention: una storia infinita*, in *Penale Diritto e procedura*, 2022.

Id., *La CGUE mette i paletti all'accesso ai dati del cellulare*, in *Altalex*, 2024.

Flor R., *Data retention ed art. 132 cod. Privacy: vexata questio?*, in *Diritto penale contemporaneo*, 2017.

Id., *La tutela dei diritti fondamentali della persona nell'epoca di internet. Le sentenze del Bundesverfassungsgericht e della Curtea Constitutionalâ su investigazioni ad alto contenuto tecnologico e data retention*, in Picotti L.-Ruggieri F. (a cura di), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica,* Giappichelli, 2011, pp. 45-46.

Flor R.-Marcolini S., *Dalla data retention alle indagini ad alto contenuto tecnologico*. Giappichelli, 2022, pp.84-89.

Fontani C., *La svolta della Consulta: la "corrispondenza telematica" è pur sempre corrispondenza*, in *Diritto penale e processo,* 10, 2023, p. 1322.

Formici G., *La data retention saga al capolinea? Le ultime pronunce della CGUE in materia di conservazione dei metadati per scopi securitari, tra conferme e nuove aperture*, in *DPCE online* (*https://www.dpceonline.it*), 1, 2021, pp. 1361, 1367.

Giangreco M., *Data retention*, acquisizione e utilizzabilità dei tabulati telefonici e telematici: una riflessione incrociata, in *Cassazione penale*, 4, 2022, pp. 1675, 1686, 1681.

Greco C., *Quest'acquisizione non s'ha da fare: ennesimo "no" della Corte di giustizia alla data retention indiscriminata in campo penale*, in *Il diritto dell'informazione e dell'informatica*, 2, 2021, pp. 237, 252-252, 254.

Griffo M., *La Corte di cassazione fissa i criteri per il sequestro dei dati informatici e telematici (prima ed a prescindere dall'intervento del legislatore), in Giurisprudenza Penale Web (https://www.giurisprudenzapenale.com), 6,* 2025.

La Rocca E.N., *A margine di una recente sentenza della Corte di giustizia UE (c-748/18): riflessi sinistri sulla disciplina delle intercettazioni in Italia*, in *Diritti Comparati,* 1, 2021,pp. 1-2, 4.

La Torre M.- Zanetti G., *Seminari di Filosofia del diritto*, Rubbettino, 2000.

Leo G., *Le indagini sulle comunicazioni e sugli spostamenti delle persone: prime riflessioni riguardo alla recente giurisprudenza europea su geolocalizzazione e tabulati telefonici*, in *Sistema penale,* 2021, p.135.

Luparia L., *Il sistema penale ai tempi dell'Internet. La figura del provider tra diritto e processo*, in Luparia L. (a cura di), *Internet provider e giustizia penale*, Giuffré, 2012, p.8.

Id., *Data retention e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, in *Diritto di Internet,* 4, 2019, pp. 762, 764.

Lupton D., *Sociologia digitale*, Pearson, 2018.

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 Web,* 3, 2022, pp. 6, 10, 21, 25, 27-43;

Malacarne, A., *Ancora sulle ricadute interne della sentenza della Corte di giustizia in materia di acquisizione di tabulati telefonici: il G.I.P. di Roma dichiara il "non luogo a provvedere" sulla richiesta del P.M*, in *Sistema Penale*, 2021.

Id., *La Cassazione sul sequestro dello smartphone: la disciplina italiana non è conforme al diritto dell'UE (…ma il materiale raccolto è comunque utilizzabile)*, in *Sistema penale,* 2025.

Marcolini S., *L'istituto della data retention tra legalità interna ed internazionale,* in Cadoppi A.-Canestrari S.-Manna A.- Papa M. (diretto da)*, Cybercrime,* Utet Giuridica, 2019*,* pp.1581, 1586..

Masera A.-Scorza G., *Internet, i nostri diritti*, Laterza, 2016.

Mucciarelli F., *Conservazione di dati di traffico di comunicazioni elettroniche e market abuse: una rilevante decisione della Corte di Giustizia dell'Unione Europe*, in *Sistema penale,* 2022.

Murro O., *Dubbi di legittimità costituzionale e problemi di inquadramento sistematico della nuova disciplina dei tabulati,* in *Cassazione penale*, 6, 2022, p. 2442.

Id., *La geolocalizzazione tramite celle telefoniche. Soluzioni percorribili, in un mondo digitale in trasformazione*, in *Diritto penale e processo,* 8, 2023, pp.1089-1090.

Id., *Prospettive in tema di sequestro dello smartphone: le novità approvate dal Senato*, in *Diritto penale e Processo*, 12, 2024, p.1619.

Neroni Rezende I. *Dati esterni alle comunicazioni e processo penale: questioni ancora aperte in tema di data retention,* in *Sistema* Penale, 5, 2020, p. 192.

Omaggio V., *I diritti oltre lo Stato. La governance europea e la crisi dei diritti*, in *Rivista di Filosofia del Diritto*, 1, 2021, p.38-39.

Id., *Ascesa e declino della democrazia costituzionale*, in *Rivista di Filosofia del Diritto*, 2, 2024, p.379.

Orrù E., *Verso un nuovo panottico? La sorveglianza digitale*, in Casadei T.-Pietropaoli S. (a cura di), *Diritto e tecnologie informatiche*, seconda edizione ampliata ed aggiornata, Wolters Kluwer, 2024, pp. 232, 238-239, 240-241, 243.

Parodi L., *La "gravità dell'ingerenza" nel prisma della proporzionalità: nuovi equilibri in tema di data retention*, in *Sistema penale,* 2025, p.18.

Perri P., *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, Giuffré Francis Lefebvre, 2020.

Pestelli *G.*, *Convertito in legge il D.L. 132/2021: le modifiche apportate (e quelle mancate) in materia di tabulati*, in *Altalex*, 18.11.2022, pp. 5-6.

Pittiruti M., *Dalla Corte di Cassazione un vademecum sulle acquisizioni probatorie informatiche e un monito contro i sequestri digitali omnibus*, in *Sistema penale*, 2021.

Ponti B., *Il rapporto tra cybersicurezza e tutela dei dati personali: sinergie, bilanciamenti e parallelismi*, in *Rivista Italiana di Informatica e Diritto*, 2, 2024, p. 151.

Rafaraci T., *Verso una law of evidence dei dati*, in *Diritto penale e processo*, 7, 2021, p.854.

Raucci P., *Le condizioni per l'accesso ai dati del cellulare per il diritto europeo*, in *Archivio penale Web*, 2, 2025.

Resta F., *La nuova disciplina dell'acquisizione dei tabulati*, in *Giustizia insieme*, 2021, pp.2-3.

Id., *La corte di giustizia europea torna ancora sulla data retention*, in *Giustizia insieme*, 2022.

Rinaldini F., *Data retention e procedimento penale. Gli effetti della sentenza della Corte di Giustizia nel caso H.K. sul regime di acquisizione dei tabulati telefonici e telematici: urge l'intervento del legislatore*, in *Giurisprudenza Penale Web*, 5, 2021, pp. 7-8.

Rodotà S., *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, 2014.

Sambuco G., *Note in tema di data retention*, in *Archivio penale Web*, 2, 2022, pp. 3-4, 9-12, 14.

Spangher G., *Conservazione dei dati e diritto alla riservatezza. La Corte di Giustizia interviene sulla data retention. I riflessi sulla disciplina interna*, in *Giustizia insieme*, 2021, p. 4.

Id., *I tabulati: il regime transitorio…in attesa degli effetti generati dallo tsunami della nuova sentenza della Corte di giustizia*, in *Giustizia insieme*, 27.4.2022.

Id., *Data retention: non basta un restyling ora serve una vera riforma organica*, in *Guida al Diritto*, 17, 2022, pp. 12-14.

Stampanoni Bassi G. (a cura di), *Acquisizione dei dati telefonici: il Tribunale di Tivoli si pronuncia sull'efficacia della sentenza CGUE del 2 marzo 2021 (C 746/18)*, in *Giurisprudenza Penale Web*, 2021.

Id. (a cura di), *Acquisizione dei tabulati telefonici: anche la Corte di Assise di Napoli esclude un'applicazione diretta della sentenza CGUE del 2 marzo 2021 (C 746/18)*, in *Giurisprudenza Penale Web*, 2021.

Id. (a cura di), *Acquisizione dei tabulati telefonici: anche la Corte di Cassazione esclude una applicazione diretta della sentenza CGUE del 2 marzo 2021 (C 746/18)*, in *Giurisprudenza Penale Web*, 2021.

Tartara V., *La Corte di Giustizia conferma il "divieto di conservazione generalizzata e indiscriminata" dei dati relativi al traffico delle comunicazioni elettroniche per finalità preventive di contrasto alla criminalità. Possibili ricadute nell'ordinamento italiano*, in *Sistema penale,* 2022, pp. 185, 194.

Tavassi L., *Acquisizione di tabulati, tutela della privacy e rispetto del principio di proporzionalità*, in *Archivio penale Web,* 2022, pp. 2, 4, 11-12.

Terolli E., *Privacy e protezione dei dati personali Ue vs. Usa. Evoluzioni di diritto comparato e il trasferimento dei dati dopo la sentenza "Schrems II"*, in *Il diritto dell'informazione e dell'informatica*, 1, 2021 pp. 51, 77.

Todaro G., *L'evoluzione delle fonti del diritto nella "società algoritmica": data retention e diritti fondamentali della persona*, in *Cassazione Penale*, 6, 2024, pp. 2016, 2036.

Tondi V., *La disciplina italiana in materia di data retention a seguito della Corte di Giustizia UE: Il Tribunale di Milano nega il contrasto con il diritto sovranazionale*, in *Sistema Penale*, 2021.

Torre F., *Data retention: una ventata di "ragionevolezza" da Lussemburgo (a margine della sentenza della Corte di giustizia 2 marzo 2021, c-746/18)*, in *Consulta online*, III , 2021, pp. 540, 543, 546, 548-550, 551-552.

Torre M., *Considerazioni su perquisizione, sequestro e intercettazioni digitali*, in *Diritto penale e processo,* 6, 2024, p. 812.

Ziccardi G., *L'odio online. Violenza verbale e ossessioni in rete*, Raffaele Cortina Editore, 2016.

Id., *Sorveglianza elettronica, data mining e trattamento indiscriminato delle informazioni dei cittadini tra esigenze di sicurezza e diritti di liberta*, in *Ragion pratica*, 1, 2018, pp. 31, 36.