RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 1/2026 • DOI 10.32091/RIID0277 • articolo sottoposto a peer review • pubblicato in anteprima il 8 lug. 2026

Silvia Bonetti

La *data retention*: alcune riflessioni nella prospettiva del diritto privato della protezione dei dati personali

Il presente contributo prende in esame, in una prospettiva di diritto privato, il ruolo dei fornitori di servizi di comunicazione elettronica nell'ambito delle investigazioni digitali, con particolare riferimento all'impiego dello strumento della *data retention*. In tale contesto, emerge chiaramente come il perseguimento di finalità pubblicistiche di lotta alla criminalità richieda necessariamente la cooperazione di operatori privati, i quali, in qualità di titolari del trattamento, assumono un ruolo centrale e altamente responsabilizzato nel garantire l'adozione di misure tecniche e organizzative adeguate a far fronte ai rischi per la sicurezza e l'integrità delle informazioni degli utenti interessati.

Data retention – Conservazione di dati personali – Acquisizione di dati personali
Princìpi applicabili al trattamento – Accountability

Data retention: some private law remarks in the light of the protection of personal data

This article analyses, from a private law perspective, the role of electronic communications service providers in the context of digital investigations, with reference to data retention. Within this framework, it clearly emerges that the pursuit of public interests in combating crime necessarily entails the cooperation of private operators, who, in their capacity as data controllers, play a central and highly responsible role in ensuring the adoption of appropriate technical and organizational measures to address risks to the security and integrity of information relating to the users concerned.

Data retention – Storage of personal data – Access to personal data
Principles relating to processing of personal data – Accountability

L'Autrice è assegnista di ricerca in Diritto privato presso il Dipartimento di Scienze Giuridiche dell'Università di Verona

Questo contributo fa parte della sezione monografica *Transizione digitale e criminalità: prospettive evolutive tra categorie sostanziali e law enforcement – Parte 2,* a cura di Gaetana Morgante e Gaia Fiorinelli

1. Introduzione: la rilevanza della *data retention* per il diritto privato della protezione dei dati personali

La *data retention*, anche se tema pressoché sconosciuto al civilista e, per contro, oggetto di ampie riflessioni nell'ambito del diritto penale e processuale penale e, precisamente, nel contesto delle investigazioni digitali[1], indubbiamente richiede di essere letta e analizzata anche nell'angolo visuale del diritto privato della protezione dei dati personali.

Lo strumento investigativo concretamente si sostanzia nell'obbligo, per i fornitori di servizi di comunicazione elettronica, di conservare per un prolungato periodo di tempo i dati (anche di natura personale) generati dall'uso di tali servizi, a cui consegue la possibilità, per l'autorità giudiziaria, di acquisirli per finalità di prevenzione, indagine, accertamento e perseguimento di reati, nonché per l'esecuzione di sanzioni penali. La sua attuazione impone, dunque, un necessario bilanciamento con i diritti fondamentali del rispetto della vita privata e della vita familiare e della protezione delle informazioni di natura personale[2].

Nella relativa disciplina trovano, però, riferimento i soli dati cc.dd. esterni del traffico delle comunicazioni elettroniche, con la conseguenza che dal suo ambito di applicazione devono ritenersi esclusi obblighi di conservazione e poteri di acquisizione che abbiano ad oggetto dati relativi al contenuto delle comunicazioni stesse, ciò che comporterebbe una eccessiva intrusione nella sfera personale dei singoli utenti.

Tale esclusione, tuttavia, non ridimensiona la portata dirompente dell'impatto di una simile disciplina nella sfera giuridica dei soggetti interessati coinvolti, poiché la conservazione e la successiva condivisione di dati – quali quelli necessari ad individuare la fonte di una comunicazione, la sua destinazione, la data, l'ora e la durata della stessa, così come la posizione geografica dei soggetti coinvolti nella conversazione –, sebbene funzionali a fare fronte a generali esigenze di pubblica sicurezza, evidentemente realizzano una significativa ingerenza nei diritti fondamentali degli individui. È pertanto inevitabile che il funzionamento della *data retention* e le garanzie che ad essa si accompagnano a tutela degli utenti delle comunicazioni elettroniche vengano inquadrati anche nella prospettiva dei princìpi che governano il diritto della protezione dei dati di natura personale[3].

1. In argomento, nella precisa prospettiva del penalista e del processual penalista, che pure è necessario comprendere per poter proporre qualche considerazione sul versante del diritto privato della protezione dei dati personali, v. almeno Flor–Panattoni 2023; Flor–Marcolini 2022; Flor 2015.
2. Ci si riferisce, in particolare, ai diritti enunciati agli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea.
3. Ma v. anche Flor–Panattoni 2023, pp. 492-494, i quali, in ragione della natura particolarmente intrusiva degli strumenti investigativi digitali (con riguardo specificamente al *lawful hacking*), individuano soprattutto nella

2. Lo statuto eurounitario della *data retention* nella elaborazione della Corte di giustizia UE: dalla sentenza *Digital Rights*...

Al fine di sviluppare il tema nella prospettiva annunciata, si rende in via preliminare necessario comprendere, sia pure per tratti essenziali, l'evoluzione storica – normativa e giurisprudenziale – della *data retention*.

Sospinto della introduzione, in numerosi ordinamenti nazionali, di discipline specifiche che individuavano, per i fornitori di servizi di comunicazione, precisi obblighi di conservazione dei dati relativi al traffico e all'ubicazione, al fine di consentire alle autorità competenti, ove necessario, di impiegarli per esigenze di pubblica sicurezza, il legislatore (allora) comunitario ha ritenuto opportuno intervenire con l'adozione di una disciplina di armonizzazione: la direttiva 2006/24/CE[4]. Tale strumento normativo si distingueva, per specialità, dalla di poco precedente direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, la quale, a sua volta, traduceva e adattava allo specifico settore di riferimento i princìpi generali dell'allora vigente direttiva 95/46/CE sulla tutela delle persone fisiche con riguardo al trattamento di dei dati personali, nonché alla libera circolazione di tali dati.

Sebbene le normative nazionali in materia di *data retention* avessero sicuramente il pregio di cogliere l'importanza dell'acquisizione di questi dati nelle azioni di contrasto alla criminalità, esse rivelavano, al contempo, un punto di debolezza nel loro carattere frammentario e disomogeneo, sul piano tanto della regolamentazione giuridica quanto della attuazione tecnica, e ciò in un settore, quello delle comunicazioni elettroniche, idoneo ad assumere una dimensione anche transnazionale, che avrebbe dovuto, perciò, trovare uniforme regolamentazione all'interno della allora Comunità (oggi Unione) europea[5].

La direttiva sulla *data retention* del 2006, che per anni è stato primo e principale strumento normativo per consentire la conservazione e la successiva acquisizione di dati nel contesto delle investigazioni digitali, diviene ben presto oggetto di uno scrutinio di legittimità da parte della Corte di giustizia, complice pure lo sviluppo di una maggiore sensibilità, anche giuridica, per la tutela delle informazioni personali a fronte della introduzione di tecnologie digitali sempre più innovative.

Nel 2014, con la pronuncia *Digital Rights*[6], la direttiva sulla *data retention* viene dichiarata invalida. Essa difetta – nella visione della Corte – di un coerente bilanciamento tra gli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, da un lato, e l'interesse generale alla lotta e alla repressione della criminalità (anche organizzata e terroristica) dall'altro. Poiché si discorre di due esigenze di protezione contrapposte, ma entrambe di rango fondamentale, le previsioni della direttiva avrebbero dovuto essere ideate di modo da far sì che la regressione di una in favore dell'altra fosse ispirata al principio eurounitario di proporzionalità, così come enunciato nell'art. 52 della Carta dei diritti fondamentali dell'Unione

cybersecurity, e non solo nella privacy e nella protezione dei dati personali, un autonomo interesse di tutela da porre in compensazione con le esigenze di pubblica sicurezza.

4. Si tratta della Direttiva riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione (nota anche come direttiva sulla *data retention* o direttiva Frattini).

5. Cfr. considerando n. 6 della direttiva 2006/24/CE, ove si osserva che le differenze tra le normative dei singoli Stati Membri "costituiscono un ostacolo al mercato interno delle comunicazioni elettroniche". Lo strumento di indagine dell'accesso ai dati conservati dai fornitori dei servizi di comunicazioni elettroniche rappresenta inoltre efficace strumento per la lotta alle forme di criminalità anche internazionale, sicché solo una disciplina armonizzata sarebbe stata in grado di massimizzare il livello di cooperazione giudiziaria in materia penale nello spazio (allora) comunitario. Per tale ultimo rilievo v. soprattutto Flor–Marcolini 2022, p. 7.

6. Cfr. Corte giust. Ue, 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights*, e i commenti di Cascione 2014 e Trucco 2014. V. pure il commento di Flor 2014.

europea[7], e che la regolamentazione del rapporto fra queste seguisse regole chiare e precise, in grado di assicurare la minima interferenza nella situazione giuridica che viene compressa per estendere lo spazio di operatività all'altra.

Diversi sono i passaggi della direttiva, che, così come emerge dalle argomentazioni della Corte, si pongono irrimediabilmente in contrasto con il principio di proporzionalità. Viene anzitutto in rilievo l'osservazione per cui l'obbligo di conservazione colpisce indistintamente tutti i dati relativi alle comunicazioni elettroniche, senza che operi alcun tipo di esclusione che, per esempio, circoscriva tale trattamento ad un determinato arco temporale, ovvero restringa la raccolta dei dati ad una precisamente individuata area geografica. Altrettanto indeterminata risulta poi la nozione di "reati gravi", con riferimento ai quali è possibile avere accesso ai dati conservati dai fornitori, la cui specificazione è demandata ai singoli ordinamenti nazionali. Non adeguatamente individuate sono, ancora, le categorie di soggetti abilitati all'accesso, quest'ultimo, peraltro, nemmeno sottoposto a precise limitazioni o subordinato all'autorizzazione di un giudice o di una autorità amministrativa indipendente. Indefiniti risultano altresì i criteri oggettivi sulla base dei quali individuare la durata esatta dell'obbligo. Da ultimo, le contestazioni della Corte sottolineano la mancanza di specifiche regole volte a garantire la sicurezza e la protezione dei dati conservati per periodi di tempo anche prolungati[8].

Al di là del mancato bilanciamento tra situazioni giuridiche tra loro in conflitto, il testo normativo risulta insoddisfacente anche – come in dottrina è stato osservato – per i numerosi rinvii ai singoli ordinamenti nazionali per la specificazione di alcuni aspetti – tutt'altro che marginali – della disciplina. Per quanto lo strumento stesso della direttiva presupponga, per sua natura, un intervento di recepimento da parte dei singoli Stati membri, l'insistito ricorso alla tecnica del rinvio con riguardo alla determinazione di profili decisivi per il concreto funzionamento della *data retention*, pare, invero, tradire il generale obiettivo di armonizzazione delle specifiche previsioni già in vigore negli ordinamenti nazionali, così vanificando la reale portata applicativa della direttiva[9].

A partire dalla pronuncia *Digital Rights*, cruciali in questa materia diventano i numerosi interventi della Corte di giustizia, che, anche con numerose pronunce successive, ha contribuito a delineare un vero e proprio statuto eurounitario sul tema della *data retention*; da questi nemmeno la presente riflessione può prescindere, e perciò se ne propongono a seguire gli snodi più rilevanti.

Quale conseguenza della invalidità della direttiva 2006/24/CE la disciplina di riferimento torna ad essere quella, più generale, di cui alla precedente direttiva 2002/58/CE (c.d. direttiva *e-privacy*), che la direttiva sulla *data retention* aveva meglio dettagliato e adeguato al contesto delle investigazioni digitali. In questo senso, confermando la collocazione della materia nell'ambito del diritto eurounitario (allora comunitario), si esprime la Corte di giustizia con la pronuncia del 21 dicembre 2016 (c.d. pronuncia *Tele2*)[10]. Principio ispiratore del legislatore della

7. A più riprese la Corte di giustizia richiama nelle proprie riflessioni in materia di *data retention* il principio di proporzionalità, come si vedrà anche in seguito in Corte giust. Ue, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, Tele2, e Corte giust. Ue, 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, *Quadrature*.
8. Più nel dettaglio sui singoli profili di incompatibilità della direttiva con il principio eurounitario di proporzionalità si soffermano Flor–Marcolini 2022, pp. 8-11.
9. V., in argomento, Flor–Marcolini 2022, p. 11, che, per tale ragione, si esprimono in termini di vuoto contenutistico della direttiva 2006/24/CE.
10. Corte giust. Ue, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2*. In aggiunta rispetto a quanto già affermato nella pronuncia *Digital Rights*, la Corte di giustizia individua qui, con maggiore precisione, tre distinti momenti, in relazione a ciascuno dei quali apposite tutele devono essere implementate affinché ogni singola disciplina nazionale possa dirsi conforme al concetto eurounitario di proporzionalità: la conservazione, l'accesso e la sicurezza nella fase di conservazione. Anzitutto, con riguardo alla fase della conservazione dei dati, si mette in luce la necessità di introdurre negli ordinamenti nazionali norme chiare, idonee a identificare con precisione *ex ante* le condizioni al sussistere delle quali sorge per i fornitori dei servizi di comunicazioni un obbligo di tale sorta. La successiva acquisizione di dati dovrà essere limitata alle sole ipotesi in cui si riveli essenziale per una adeguata lotta alla criminalità grave, concetto questo che dovrà essere adeguatamente specificato

direttiva *e-privacy* – osservano i giudici di Lussemburgo – è senza dubbio quello della riservatezza dei dati, sicché la *data retention*, che – come detto – prende la forma di obblighi di conservazione e comunicazione, è da collocarsi nell'ambito delle limitazioni a tale principio, precisamente individuate, nel testo della direttiva, all'art. 15. Segnatamente, si prevede che la regola relativa alla riservatezza delle comunicazioni, l'obbligo di cancellazione o anonimizzazione dei dati del traffico una volta venuta meno la finalità di trasmissione della comunicazione, così come l'anonimizzazione dei dati relativi all'ubicazione (diversi dai dati del traffico), possano essere oggetto di limitazione, da parte di una normativa nazionale, quando tale limitazione sia da considerarsi misura necessaria, opportuna e proporzionata nei settori della "sicurezza nazionale […], della difesa, della sicurezza pubblica", ovvero "per la prevenzione, ricerca, accertamento e perseguimento dei reati"[11].

Lo stato più avanzato delle elaborazioni eurounitarie in materia di *data retention* lo si raggiunge soltanto il 6 ottobre 2020, con la sentenza *Quadrature*[12]. Ribadite le affermazioni già enunciate nelle precedenti pronunce *Digital Rights* e *Tele2*, i giudici di Lussemburgo sviluppano l'operatività del principio di proporzionalità intorno a tre distinti fattori: la variabile intensità della interferenza nei diritti fondamentali dell'individuo; la gravità del fenomeno criminoso che si intende combattere; la qualità e la quantità delle garanzie che il legislatore nazionale adotta.

All'esito della valutazione di proporzionalità, che tiene conto di tali tre elementi, può risultare una interferenza di minima entità nel bene riservatezza, la quale è perciò da dirsi compatibile con la lotta contro ogni forma di criminalità, non necessariamente grave[13]; per converso, solo l'esigenza pubblica di perseguire crimini di più elevata gravità giustifica una maggiore intrusione nella sfera privata degli individui. Una regola (l'art. 15 della direttiva 2002/58/CE), che si pone come eccezionale rispetto alla tutela dei diritti fondamentali e che potenzialmente coinvolge il trattamento di un numero significativo di dati, non potrà, infatti, prescindere da criteri rigorosi che ne regolano il bilanciamento con la riservatezza e la protezione delle informazioni. Di conseguenza, non sarà sufficiente a legittimare la conservazione e l'acquisizione di dati (anche) personali la generica finalità di prevenzione e contrasto alla criminalità; piuttosto, soltanto la repressione di forme di criminalità che possano definirsi gravi potrà giustificare una più ampia compressione dei diritti dell'individuo. E, in ogni caso, tale compressione andrà accompagnata da garanzie procedurali che possano mitigare gli effetti negativi che in ipotesi si potranno riversare sugli utenti.

Fondamentale garanzia, di cui i giudici di Lussemburgo promuovono l'implementazione, è quella del modello di conservazione mirata dei dati delle comunicazioni (o t*argeted retention*)[14]. Prevedere un obbligo di conservazione generalizzata e indifferenziata dei dati di tutti coloro che

per il tramite del preciso riferimento alle singole fattispecie di reato che siano a questo riconducibili. L'accesso dovrà inoltre essere subordinato al preventivo controllo da parte di una autorità giudiziaria o amministrativa indipendente. La sicurezza dei dati conservati, infine, andrà realizzata mediante l'introduzione dell'obbligo per i fornitori di adottare, durante il periodo di conservazione, degli standard di protezione elevati, che impongano loro, allo scadere del periodo di tempo di riferimento, la cancellazione irreversibile delle informazioni raccolte.

11. Cfr. art. 15, par. 1, della direttiva 2002/58/CE.
12. Corte giust. Ue, 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, *Quadrature*.
13. Conclusione, questa, già raggiunta dalla Corte con la sentenza *Ministerio Fiscal*. Cfr. Corte giust. Ue, 2 ottobre 2018, causa C-207/16.
14. Sulla conservazione targhettizzata v., in particolare, Corte giust. Ue, 5 aprile 2022, causa 140/20, *Commissioner*, ove si ribadisce nuovamente il rapporto tra regola ed eccezione in materia di *data retention*, lì dove la regola si identifica nella cancellazione o anonimizzazione delle informazioni per le quali le finalità del trattamento possano dirsi raggiunte ed esaurite ed è, invece, eccezionale la loro ultra-conservazione. Si critica dunque, anche in questa successiva pronuncia, l'impostazione che fa discendere dalla disciplina della *data retention*, quale strumento investigativo di contrasto alla criminalità grave, obblighi di conservazione generali e indifferenziati. Per contro, se la conservazione generalizzata è da considerarsi inaccettabile in una società democratica, i modelli di

utilizzano mezzi di comunicazione elettronica significherebbe, nella sostanza, estendere nel tempo il loro trattamento, o comunque realizzarne uno nuovo, senza limitazione alcuna, in deroga al rapporto regola-eccezione, così come individuato nella direttiva *e-privacy*, e in contrasto pure con l'esigenza, di segno opposto, di contenere entro i limiti della ragionevolezza la regressione di un diritto fondamentale a fronte dell'interesse generale alla sicurezza pubblica.

Fra i criteri idonei a limitare la conservazione che la Corte espressamente suggerisce vi sono il criterio geografico, che circoscrive la raccolta dei soli dati che sono localizzabili in una determinata area ad alto rischio di criminalità; il criterio personale, che consente di identificare quelle categorie di soggetti o quei singoli soggetti che rivelino una stretta connessione con forme di criminalità grave o che, in prima persona, costituiscono una minaccia per la sicurezza; e il criterio temporale, che limita la conservazione ad un determinato periodo di tempo, allo scadere del quale la regola generale, ossia quella della cancellazione o anonimizzazione dei dati, nuovamente si riespande[15].

Si delineano così, modellati dal formante giurisprudenziale, i princìpi che devono permeare ogni disciplina, anche nazionale, in materia di *data retention*.

3. (Segue)... alla rinnovata disciplina nel diritto italiano: l'art. 132 del Codice in materia di protezione dei dati personali

Esaminati, per sommi capi, i princìpi fissati dal diritto eurounitario, occorre ora assumere una prospettiva di diritto interno e analizzare la disciplina in materia di *data retention* che il legislatore italiano, in forza della riserva concessagli dall'art 15 della direttiva *e-privacy*[16], ha introdotto.

La fonte principale che, nell'ordinamento interno, regola gli obblighi in capo agli *internet service provider* di conservare i dati (ma non il contenuto) del traffico telefonico e telematico, nonché le modalità di acquisizione di tali dati da parte delle autorità di pubblica sicurezza, è

conservazione mirata (basata, per esempio, su persone o luoghi) e rapida (o *quick freeze*), si rivelano funzionali alle esigenze di indagine senza tradursi in una eccessiva compressione del diritto alla riservatezza. È dunque, in sintesi, vietata, per finalità di lotta alla criminalità grave e di prevenzione a minacce gravi per la sicurezza pubblica, la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione. Se posta in essere per le medesime finalità, non è invece in contrasto con il diritto eurounitario una disciplina nazionale che preveda la conservazione generalizzata e indifferenziata degli indirizzi IP attribuiti all'origine di una connessione, purché essa sia limitata nel tempo e allo stretto necessario; parimenti ammessa è la conservazione generalizzata e indifferenziata dei dati relativi all'identità degli utenti delle comunicazioni elettroniche. Sulla selezione dei dati oggetto di conservazione riflettono anche Corte giust. Ue, 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, *Quadrature*; Corte giust. Ue, 30 gennaio 2024, causa C-118/22, *Direktor* commentata da Grillo 2024, p. 832 ss., nonché Corte giust. Ue, 28 novembre 2024, causa C-80/2023, *Ministerstvo na vatreshnite raboti*.

15. Richiama tali criteri Corte giust. Ue, 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, *Quadrature*. Anche quando oggetto di conservazione siano categorie particolari di dati personali (nella specie, dati genetici e biometrici), il relativo trattamento – sempreché sia posto in essere alle condizioni enucleate dalla giurisprudenza eurounitaria – non perde di liceità, poiché si riconosce che tali dati possano rivelarsi utili per ulteriori fini di pubblica sicurezza. Ciò che invece è da scongiurare è una raccolta sistematica e indiscriminata di tali informazioni, poiché in contrasto anche con il principio di minimizzazione, il cui rispetto, con riferimento alla conservazione di particolari categorie di dati, è da sottoporre ad un controllo ancor più rigoroso. In argomento v. Corte giust. Ue, 30 gennaio 2024, causa C-118/22, *Direktor*.

16. Restrizioni del diritto della protezione dei dati personali del medesimo tenore di quelle introdotte con la direttiva del 2002 sono oggi previste anche all'interno del GDPR, ove – all'art. 23 – si prevede che possa essere circoscritta, mediante apposita misura legislativa, la portata degli obblighi e dei diritti del Regolamento, così come dei princìpi generali in materia di trattamento dallo stesso individuati "qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare […] la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica".

l'art. 132 del d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali).

La norma, pur presente già nel testo originario del Codice del 2003, prende atto delle elaborazioni della giurisprudenza eurounitaria soltanto nel 2021[17], a seguito della pronuncia *Prokuratuur*[18], con un mirato intervento legislativo che ha voluto adeguare – sebbene con qualche ritardo – la disciplina interna sulla *data retention* ai princìpi formulati dalla Corte di giustizia[19].

Nonostante tale intervento abbia sicuramente il merito di avere attenuato i profili di contrasto con il diritto eurounitario, esso non pare del tutto sciogliere alcune criticità che – per quel che in questa sede più rileva – si riflettono anche sul diritto privato della protezione dei dati personali.

La disciplina interna, nella sua formulazione attuale, chiarisce anzitutto i tempi di conservazione dei dati, distinguendo tra dati di traffico telefonico e dati di traffico telematico. Quale regola generale, così come individuata al comma 1, i primi sono conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione dei reati. I secondi (con la precisazione che non sono, fra questi, inclusi i dati relativi al contenuto delle comunicazioni) sono, per le medesime finalità, conservati dal fornitore per dodici mesi dalla data della comunicazione[20]. La norma precisa poi, al comma 1-*bis*, che i dati relativi alle chiamate senza risposta, trattati temporaneamente da parte dei fornitori, che siano accessibili al pubblico oppure di una rete pubblica di comunicazione, sono conservati per trenta giorni.

Tale disciplina deve essere, però, letta unitamente a quella di cui alla l. 20 novembre 2017, n. 167[21], che, all'art. 24, prevede, per la finalità di "garantire strumenti di indagine efficace in considerazione delle straordinarie esigenze di lotta contro il terrorismo", un termine di conservazione ben più elevato, pari a settantadue mesi, dei dati del traffico telefonico e telematico, nonché dei dati relativi alle chiamate senza risposta. Quale esito del coordinamento di tali due previsioni normative, in ragione della considerazione per cui non è possibile per il fornitore conoscere con anticipo, al momento della conservazione, quale sarà la fattispecie di rilevanza penale in funzione della quale l'autorità domanderà l'accesso, il termine di settantadue mesi assorbe inevitabilmente le limitazioni temporali più brevi individuate nel Codice in materia di protezione dei dati personali, sicché il *provider* non avrà altra scelta se non quella di conservare generalmente e indistintamente tutti i dati per il periodo più lungo individuato dalla legge del 2017[22].

Sul tema dell'individuazione dell'autorità a cui compete impartire l'ordine di acquisizione dei dati è direttamente intervenuta la già ricordata riforma del

17. Le modifiche all'art. 132 del Codice in materia di protezione dei dati personali in commento vengono introdotte mediante il d.l. 30 settembre 2021, n. 132, convertito con modificazioni dalla l. 23 novembre 2021, n. 178.
18. Cfr. Corte giust. Ue, 2 marzo 2021, C-746/2018, *Prokuratuur*. V. anche il commento di Landolfi 2021, p. 1481 ss.
19. Si tratterà, nelle pagine a seguire, dell'art. 132 del Codice in materia di protezione dei dati personali nella sua attuale formulazione. Per un'analisi del testo della norma nella sua versione precedente all'intervento legislativo del 2021, v. Flor–Marcolini 2022, p. 89 ss., che ne osservano le criticità relative principalmente ai tempi di conservazione, alle modalità di acquisizione (e all'intervento del pubblico ministero), e alle finalità di accertamento e repressione dei reati.
20. In considerazione del ruolo preponderante che le nuove tecnologie della comunicazione stanno oggigiorno assumendo, a discapito della comunicazione telefonica tradizionale, difficilmente si comprende la ragione per cui il termine di conservazione dei dati del traffico telematico sia sensibilmente inferiore a quello previsto per i dati del traffico telefonico. Così anche Flor–Marcolini 2022, p. 91.
21. Il comma 5-*bis* dell'art. 132 fa infatti salva l'applicabilità della l. 20 novembre 2017, n. 167 e, in particolare, del suo art. 24.
22. In senso critico rispetto a tale irragionevole, seppure inevitabile, conclusione si esprimono, tra gli altri, Demartis 2022, p. 303 e Flor–Marcolini 2022, p. 46 s. e 89 ss. Anche una verifica *ex post*, al momento dell'accesso, della correttezza del termine di conservazione comporterebbe problemi pratici non indifferenti, per esempio, nell'ipotesi in cui la trasmissione e l'acquisizione abbiano luogo nonostante sia ormai trascorso il tempo di conservazione previsto per il reato perseguito e siano, di conseguenza, da ritenersi illegittime. Di riflesso, nella prospettiva privatistica, i trattamenti sarebbero da considerarsi illeciti poiché posti in essere in

2021[23]. Sino al 2021 i dati venivano acquisiti presso il fornitore con decreto motivato del pubblico ministero, eventualmente anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa o delle altre parti private. Nella versione attuale della norma si prevede, invece, che i dati siano acquisiti soltanto previa autorizzazione rilasciata dal giudice con decreto motivato, su richiesta del pubblico ministero o su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa o delle altre parti private, così garantendo l'imparzialità di colui che impartisce l'ordine rispetto alle finalità d'indagine[24]. La violazione di tali modalità di acquisizione, peraltro, è direttamente sanzionata dalla norma, che sancisce l'inutilizzabilità dei dati raccolti in assenza di autorizzazione (art. 132, comma 3-*quater*).

Anche i presupposti per l'acquisizione sono mutati a seguito dell'intervento legislativo del 2021, che, nello specifico, ha meglio precisato le categorie di reati con riferimento alle quali è possibile, per l'autorità competente, avere accesso ai

violazione di quella norma di legge nazionale (l'art. 132) che individua e definisce l'interesse pubblico da addurre come base giuridica ai sensi dell'art. 6, par. 1, lett. e), del GDPR.

23. In argomento i giudici di Lussemburgo sono intervenuti a più riprese. Segnatamente, Corte giust. Ue, 8 aprile 2014 cause riunite C-293/12 e C-594/12, *Digital Rights* ha sin da subito chiarito che le categorie di soggetti abilitati all'accesso devono essere precisamente individuate e che l'acquisizione deve, in ogni caso, essere subordinata all'autorizzazione di un giudice o di una autorità amministrativa che possa qualificarsi come indipendente. Così anche Corte giust. Ue, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2*. In seguito, anche Corte giust. Ue, 2 marzo 2021, causa C-746/18, Prokuratuur specifica ulteriormente il ruolo del pubblico ministero nell'accesso ai dati conservati. Sebbene, infatti, la richiesta di accesso ragionevolmente provenga da costui, che – come noto – rappresenta l'autorità titolare dei poteri investigativi e ha il ruolo di coordinare le indagini, essa dovrà essere vagliata da una autorità (giudiziaria o amministrativa) in una posizione di terzietà, che non abbia, in altri termini, un interesse diretto alla conoscenza dei dati. Il pubblico ministero, infatti, in ragione del ruolo processuale di cui è investito e della sua qualità di titolare di obblighi investigativi, non riveste una posizione di imparzialità e, per tale ragione, la sua domanda di accesso dovrà essere esaminata da un organo che sia terzo ed estraneo alla dinamica processuale. Anche secondo Corte giust. Ue, 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, *Quadrature* il trattamento deve sempre avere luogo sotto il controllo di un giudice o di una autorità amministrativa indipendente che possa verificare il rispetto delle condizioni legittimanti una estesa conservazione delle informazioni. Da ultimo, anche la più recente Corte giust. Ue, 5 aprile 2022, causa 140/20, *Commissioner* ribadisce che l'organo di polizia, seppure centralizzato e di comando, dal quale proviene la richiesta di accesso ai dati, non ha, per sua natura, i requisiti di terzietà e indipendenza che l'autorità di controllo dovrebbe invece possedere.

24. Tuttavia, in via eccezionale, quando ricorrono ragioni di urgenza e vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini, ovvero alle ricerche di un latitante, il pubblico ministero dispone la acquisizione dei dati con decreto motivato. Questo è comunicato immediatamente, e comunque non oltre quarantotto ore, al giudice competente per il rilascio dell'autorizzazione in via ordinaria. Il giudice, nelle quarantotto ore successive, decide sulla convalida con decreto motivato (art. 132, comma 3-*bis*). Da segnalare, a margine della presente riflessione, è anche la recente introduzione del comma 3-*bis*.1, quale norma di coordinamento inserita dal d.lgs. 30 dicembre 2025, n. 215, che attua il Regolamento (UE) 2023/1543 relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive a seguito di procedimenti penali. Tale disciplina si propone l'obiettivo di facilitare e accelerare l'accesso alle prove elettroniche utilizzate per indagare e perseguire i reati, indipendentemente dall'ubicazione dei dati, prevedendo che un'autorità giudiziaria in uno Stato membro dell'Unione possa richiedere allo stabilimento designato di un prestatore di servizi o ai suoi rappresentanti legali nominati in un altro Stato membro di produrre prove elettroniche (quali i dati degli abbonati, gli indirizzi del protocollo internet (IP) necessari a identificare un utente, e-mail, testi e messaggi in-app), ovvero di conservare (per un periodo di 60 giorni, prorogabile di ulteriori 30) i dati specifici in attesa di una futura richiesta di produzione. Allo scadere di tale periodo l'obbligo di conservazione cessa, a meno che l'autorità non abbia emesso un ordine di produzione relativo a quei medesimi dati.

dati conservati. Se, infatti, prima della riforma, i dati potevano essere acquisti per l'accertamento e la repressione dei reati, senza alcuna precisazione ulteriore circa le categorie di fattispecie penali che, in ragione della loro gravità e del bene giuridico protetto, giustificavano una significativa ingerenza nei diritti fondamentali dell'individuo, dal 2021, i dati possono essere acquisiti, ai sensi del comma 3, soltanto se sussistono sufficienti indizi di reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, determinata a norma dell'art. 4 cod. proc. pen.[25]

È introdotto inoltre un filtro selettivo in grado di limitare ulteriormente l'acquisizione, la quale è oggi subordinata anche alla presenza del c.d. *fumus commissi delicti*, ossia, in altri termini, alla sussistenza di sufficienti indizi di reati (fra quelli che rientrano nelle categorie individuate dalla norma) che possano giustificare l'intrusione nella sfera privata degli individui.

Sulla conformità della normativa italiana ai princìpi elaborati dalla giurisprudenza eurounitaria in materia di *data retention* riflette una recente pronuncia della Corte di giustizia del 2024, che, per la prima volta, è chiamata ad affrontare una questione di legittimità sollevata con riferimento all'art. 132 nella sua attuale formulazione[26].

Confermata quale condizione per l'acquisizione dei dati relativi al traffico telefonico e telematico l'autorizzazione di un giudice o di una autorità amministrativa indipendente[27], il ragionamento dei giudici di Lussemburgo si sofferma sulla nozione di "reato grave" adottata dal legislatore nazionale. Questa, che si basa su un limite edittale massimo *ex ante* individuato dalla legge, viene ritenuta legittima perché fondata su di un criterio oggettivo. In altri termini, una soglia fissata con riferimento alla pena della reclusione non inferiore nel massimo a tre anni non appare – nella prospettiva della Corte – eccessivamente bassa rispetto alla finalità di evitare che l'accesso ai dati da parte delle autorità diventi la regola e trascenda, dunque, l'ambito delle eccezioni[28]. Peraltro, gli stessi giudici promuovono la verifica di requisiti aggiuntivi che, unitamente ai parametri di selezione già evocati dalla norma, dovrebbero essere in grado di inverare l'idea di proporzionalità. Precisamente, occorre appurare la sussistenza di indizi di reati che rientrano nella individuata nozione di "reato grave" (come previsto dallo stesso art. 132, al comma 3); la rilevanza dei dati richiesti per l'accertamento dei fatti, mediante un c.d. test di necessità; e la possibilità per l'autorità di negare l'accesso, se richiesto nel contesto di un'indagine per reati manifestamente non gravi[29].

25. Ovvero se sussistono sufficienti indizi di reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi, ove rilevanti per l'accertamento dei fatti.
26. Si tratta di Corte giust. Ue, 30 aprile 2024, causa C-178/22, *Procura della Repubblica presso il Tribunale di Bolzano*.
27. Motivo principale, questo, per cui il legislatore italiano – come anticipato – era già intervenuto del 2021, individuando nell'autorizzazione giudice, e non più nel decreto pubblico ministero, il provvedimento che legittima l'accesso ai dati.
28. Però, non a torto si è osservato che, facendo corrispondere all'idea di "reato grave" tutte le fattispecie penali i cui limiti edittali rientrano nei limiti della previsione introdotta dal legislatore del 2021, quelle che, per contro, ne rimangono escluse sono di minima rilevanza, ciò che non consentirebbe, a ben vedere, di circoscrivere nemmeno l'acquisizione entro i confini della proporzionalità, come da tempo auspica la Corte Ue (v. soprattutto Corte giust. Ue, 5 aprile 2022, causa 140/20, *Commissioner*). In senso critico rispetto a tale scelta legislativa v. Flor–Marcolini 2022, p. 54 s., ad avviso dei quali la previsione in commento "non può minimamente soddisfare", poiché essa "dà l'illusione di aver effettuato una delimitazione del perimetro delle violazioni, ma in realtà non lascia fuori che le contravvenzioni e pochi delitti di davvero infima gravità". Nemmeno è da trascurare che il concetto stesso di "reato grave", non trovando una sua precisa enunciazione nell'ambito del diritto eurounitario, è destinato a mutare in ragione delle diverse considerazioni e valutazioni di ciascuno Stato membro, con l'esito che le fattispecie penali per la repressione delle quali è consentito conservare e acquisire informazioni di natura personale saranno sicuramente differenti nei singoli ordinamenti nazionali. Ne deriva il concreto rischio di lasciare spazio ad applicazioni elusive dell'art. 15 della Direttiva *e-privacy* e così, di riflesso, si profilano margini per una inauspicata e indebita ingerenza nei diritti fondamentali degli individui.
29. L'autorità indipendente deve, infatti, avere sempre la possibilità di intervenire al fine di riequilibrare, se vi è necessità, il bilanciamento tra le esigenze di natura investigativa, da un lato, e i diritti fondamentali alla riservatezza e alla protezione dei dati personali, dall'altro.

Ad una conservazione generalizzata e indifferenziata (e protratta per un periodo di tempo molto esteso) segue, dunque, un (eventuale) accesso solo a condizione che questo superi un vaglio di necessità che ha riguardo alla stretta rilevanza di quei dati per esigenze di lotta alla criminalità grave e alla proporzionalità dell'acquisizione stessa agli interessi pubblici nel concreto perseguiti.

L'art. 132 sembra allora collocare il momento selettivo dei dati nella sola fase della "consegna" di questi all'autorità, dando per implicita una preliminare conservazione generalizzata[30]. La novella del 2021 non ha, infatti, introdotto alcun profilo di novità con riferimento alle categorie di dati conservati e rimane ferma su di un modello di conservazione generalizzato ed indifferenziato, che non pone alcuna limitazione in ordine alle categorie di dati che devono essere trattenuti dal fornitore. Ne consegue un incremento esponenziale del rischio di lesione del diritto alla riservatezza e alla protezione dei dati personali, anziché una sua contemperazione; e ciò a dispetto delle indicazioni della giurisprudenza eurounitaria che, all'opposto, promuovono – come detto – criteri idonei a limitare anche la conservazione (e non solo l'accesso, peraltro successivo e solo eventuale) alle sole informazioni strettamente necessarie per far fronte ad esigenze di pubblica sicurezza, sul modello della conservazione selezionata[31].

4. Il ruolo del diritto della protezione dei dati personali nella conservazione e acquisizione di informazioni per finalità di contrasto alla criminalità: profili di criticità

I profili segnalati, a ben vedere, denunciano ancora un qualche margine di incompatibilità della disciplina interna sulla *data retention* non solo con lo statuto elaborato in materia dalla Corte di giustizia, ma anche con il diritto della protezione dei dati personali, come ora si tenterà di chiarire[32].

Il parametro normativo a cui riferirsi per valutare tale (in)compatibilità è rappresentato dalla direttiva (UE) 2016/680 (nota anche come *Law Enforcement Directive* o, più brevemente, direttiva LED, attuata nel nostro ordinamento con il d.lgs. 18 maggio 2018, n. 51), ma anche – e forse soprattutto – dal Regolamento (UE) 2016/679, più comunemente noto come GDPR (o RGPD, nella versione italiana).

Come già si è avuto modo di ricordare, sono due i trattamenti in cui le misure di *data retention* si sostanziano: il primo, rappresentato dalla conservazione, per determinati periodi di tempo (anche prolungati), dei dati (anche) personali da parte del fornitore dei servizi di comunicazione elettronica; il secondo, temporalmente e logicamente successivo al primo, che ha luogo con l'acquisizione da parte dell'autorità giudiziaria dei dati necessari al perseguimento delle finalità di pubblica sicurezza da questa addotte a fondamento della propria richiesta. Ora, mentre del secondo trattamento è indubbiamente titolare l'autorità competente, che provvederà alla individuazione di determinate finalità per le quali i dati devono essere acquisiti, specificando le più generali esigenze di prevenzione, indagine, accertamento e repressione di reati dei quali già sussistano sufficienti indizi, la conservazione delle informazioni compete, invece, ad un soggetto privato, il *provider* del servizio di comunicazione elettronica. Questi, invero, non determina autonomamente le finalità e i mezzi di tale trattamento; esse, piuttosto, sono *ab origine* individuate dal diritto eurounitario (art. 15, direttiva *e-privacy*) e dal diritto nazionale (art. 132 Codice in materia di protezione dei dati personali), che del primo costituisce attuazione. Non è però di ostacolo alla qualificazione di un soggetto come titolare del trattamento il fatto che questi lo ponga in essere per finalità e mezzi che sono individuati

30. Alla medesima conclusione giungono anche Flor–Marcolini 2022, p. 109.

31. Cfr., in particolare, le già citate Corte giust. Ue, 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, *Quadrature*, e Corte giust. Ue, 5 aprile 2022, causa 140/20, *Commissioner*, ove vengono suggerite e ampiamente descritte misure di c.d. *targeted retention*.

32. Per un'analisi delle residue criticità in ambito penale e processuale penale v. diffusamente Flor–Marcolini 2022, p. 107 ss. e Demartis 2022, p. 306 s., che in particolare si sofferma sull'assenza di una disciplina dedicata ai dati di ubicazione, che possono entrare nella disponibilità del *provider* anche in assenza di traffico telefonico e telematico.

direttamente dalla legge, ai sensi dell'art. 4, n. 7), secondo periodo, GDPR[33].

Di conseguenza, soltanto con riferimento al secondo trattamento (acquisizione dei dati oggetto di previa conservazione) dovrebbe trovare applicazione la direttiva LED, il cui ambito di operatività è limitato ai trattamenti di dati personali posti in essere dalle "autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica"[34]. Di contro, il trattamento che consiste nella conservazione sembra rientrare nella sfera applicativa del GDPR e delle tutele – più elevate rispetto a quelle della direttiva LED – che esso individua a protezione dei soggetti interessati e delle informazioni personali che li identificano o li rendono identificabili[35].

Occorre, dunque, osservare criticamente la fase della conservazione dei dati nel prisma dei princìpi che ne governano il trattamento secondo le previsioni del GDPR e non alla luce della, sia pure simile, disciplina della direttiva LED.

L'immediato esito di tale riflessione è rappresentato dalla considerazione per cui la soluzione del legislatore italiano, che sposta dalla conservazione all'accesso il momento di selezione dei dati, rischia di entrare in aperto conflitto anzitutto con il principio di minimizzazione, che va interpretato nel senso più rigoroso di cui al GDPR[36]. Se infatti il trattamento che consiste nella acquisizione dei dati deve rientrare entro il già ricordato parametro dalla nozione di "reato grave" e il filtro selettivo è rappresentato dalla sussistenza di indizi di tali reati, la conservazione avviene invece – come detto – in modo generalizzato, senza che abbia spazio alcun tipo di vaglio preliminare che consenta di parametrare alle finalità del trattamento i dati raccolti. La minimizzazione non pare certamente in linea con una raccolta generalizzata e indifferenziata di informazioni relative al traffico delle comunicazioni telefoniche e telematiche, senza che – come a più riprese suggerito dalla stessa Corte di giustizia – vengano adottati criteri idonei a circoscrivere – nello spazio, nel tempo, o in base ad altre valutazioni – le categorie di dati che devono essere sottratte alla regola generale della cancellazione o anonimizzazione, per fare fronte a finalità ulteriori di sicurezza pubblica. La mancata implementazione di misure di conservazione targhettizzata, in altre parole, non soltanto è pratica in contrasto con il principio eurounitario della proporzionalità, ma nemmeno sembra essere fedele all'esigenza di custodire, in vista di una eventuale acquisizione, solo i dati che siano adeguati, pertinenti e limitati a quanto necessario per le finalità (speciali) per le quali possono essere oggetto di ulteriore trattamento[37].

33. Sul punto riflette anche la stessa Corte di giustizia, secondo cui per attribuire la qualità di titolare del trattamento ad una entità, ai sensi dell'articolo 4, n. 7, secondo periodo, del GDPR non è necessario che tale entità eserciti un'influenza sulla determinazione delle finalità e dei mezzi di tale trattamento, previste, invece, dallo stesso diritto nazionale. Cfr. Corte giust. Ue, 27 febbraio 2025, causa C-638/23, *Amt der Tiroler Landesregierung*.

34. Cfr. art. 1, par. 1, della direttiva.

35. A meno che non si voglia considerare l'idea che le peculiari finalità che con la conservazione ci si propone di perseguire non siano idonee ad attrarre nella sfera di applicabilità della direttiva LED anche il primo trattamento.

36. Il principio è enunciato dal GDPR, all'art. 5, par. 1, lett. c), ma è presente anche nella direttiva (UE) 2016/680, nel suo art. 4, par. 1, lett. c), nell'ambito della quale esso deve essere valutato in misura attenuata in ragione delle finalità dei trattamenti che rientrano nel suo ambito d'applicazione. In generale, sul principio di minimizzazione, v. almeno Battistini–Matarazzo–Zanetti 2023, p. 231 ss.; Roßnagel–Richter 2023, p. 279 ss.; Dell'Utri 2019, p. 179 ss. e 209 ss.; Colapietro–Iannuzzi 2017, p. 106 ss.

37. Il principio di minimizzazione è da mettere in connessione con il principio di proporzionalità, di cui è espressione l'art. 52 della Carta dei diritti fondamentali dell'Unione europa. Mentre la proporzionalità, nel contesto della protezione dei dati personali, persegue l'obiettivo primario di contenere entro limiti minimi le lesioni di tale diritto fondamentale, compresso per lasciare più ampia operatività ad un diritto di pari rango, e perciò opera *ex ante* sul piano della selezione della finalità che mediante il trattamento possono soddisfare tale diritto, la minimizzazione, di contro, viene in rilievo in un momento logicamente e temporalmente successivo,

Ulteriori profili di contrasto emergono anche con il principio di integrità e riservatezza del trattamento[38]: in un simile assetto il potenziale rischio per gli utenti è, infatti, incrementato dalla mancata individuazione, all'interno del testo normativo, di precise misure volte all'adozione di standard elevati di protezione[39].

Il concetto di rischio evoca, dunque, un ulteriore rilevante profilo problematico della disciplina italiana sulla *data retention*; profilo, questo, che, peraltro, rappresenta – come si vedrà – uno dei punti di contatto più evidenti tra la riflessione di diritto penale sostanziale e processuale e l'ambito privatistico della protezione dei dati personali.

Il generico richiamo, con l'art. 132-*ter*, all'art. 32 del GDPR, ha sicuramente inteso estendere, anche a tale ambito, le previsioni in materia di sicurezza del Regolamento, ma, nel farlo, il legislatore ha omesso di identificare misure di protezione (anche minime) da cui non poter prescindere, che sarebbero state certamente utili all'operatore privato per far fronte ad un rischio certamente elevato sia in ragione della indiscriminata raccolta di informazioni e della loro conservazione per un periodo di tempo molto esteso sia in considerazione delle conseguenze negative di cui pure le esigenze di lotta alla criminalità risentirebbero in ipotesi di violazione dei dati.

Posto che, in ogni caso, al trattamento che consiste nella conservazione dei dati da parte del *provider* pare debba applicarsi il GDPR (e non la direttiva LED), il mancato riferimento a specifici profili di sicurezza non potrebbe trovare giustificazione nel diverso rapporto tra il diritto alla protezione dei dati personali dei soggetti interessati e le finalità di pubblica sicurezza perseguite con il trattamento che costituiscono l'ambito di operatività della direttiva del 2016. Sebbene, infatti, dette finalità rendano leciti periodi di conservazione prolungati ed ammettano la raccolta di elevate quantità di informazioni, con la conseguenza che i diritti dei soggetti interessati possono risultare compressi, l'ambito della sicurezza – così come previsto nella direttiva – non pare subire alcuna restrizione rispetto a quanto previsto dalla disciplina generale in materia di protezione dei dati personali[40]. Al contrario, in ragione di un livello di rischio che è, per natura, elevato, il principio di integrità e riservatezza dei dati personali dovrebbe trovare, nell'ambito che ci occupa, un primario campo di applicazione.

Risulta così essenziale l'individuazione di precise ed efficaci misure di sicurezza, che, nella loro applicazione concreta, sono da considerarsi direttamente funzionali ad inverare – sia nella fase di conservazione sia in quella di accesso ai dati del traffico telefonico e telematico – anche il principio di proporzionalità, nel suo senso di minor ingerenza possibile – mediante l'adozione di adeguate garanzie – nella situazione giuridica compressa in favore di quella che, all'esito di un bilanciamento, è da tutelare in via preminente.

Di tale individuazione viene investito il singolo *provider*, a cui competerà la scelta e l'attuazione

per circoscrivere il trattamento ai soli dati adeguati, pertinenti e limitati alle finalità che già sono state oggetto di bilanciamento (v. sul punto Roßnagel–Richter 2023, p. 281). Un trattamento che ignori le esigenze di minimizzazione risulterà, perciò, in conflitto anche con il principio di proporzionalità.

38. Cfr. art. 5, par. 1, lett. f), GDPR (richiamato anche dall'art. 4, par. 1, lett. f) della direttiva LED).

39. Già a partire da Corte giust. Ue, 8 aprile 2014 cause riunite C-293/12 e C-594/12, *Digital Rights,* la Corte europea ha affermato la necessità di adottare specifiche regole volte a garantire la sicurezza e la protezione dei dati raccolti. Corte giust. Ue, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2*, ha in seguito ribadito che la sicurezza dei dati conservati deve essere implementata mediante l'introduzione dell'obbligo per i *provider* di adottare, durante il periodo di conservazione, degli standard di protezione elevati e, al contempo, con l'imposizione, allo scadere del periodo di tempo di riferimento, della cancellazione irreversibile delle informazioni. Ha precisato, infine, Corte giust. Ue, 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, *Quadrature*, che la compressione dei diritti dell'individuo a fronte di interessi generali di contrasto alla criminalità grave deve essere accompagnata da garanzie procedurali idonee a mitigare la lesione dei diritti fondamentali degli utenti.

40. Cfr., in particolare, l'art. 29 della direttiva, di cui l'art. 16 del d.lgs. 18 maggio 2018, n. 51 rappresenta attuazione, ove è previsto – sulla scorta del modello del GDPR – che il titolare del trattamento (e il responsabile del trattamento), "tenuto conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, mettano in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio".

degli strumenti più idonei a contenere i rischi che incombono sui diritti e le libertà fondamentali dei soggetti interessati, avvalendosi degli strumenti che il GDPR stesso mette a disposizione.

Al pari di qualsiasi titolare del trattamento, anche il fornitore di servizi di comunicazione elettronica che sia tenuto, ai sensi dell'art. 132, ad ultra-conservare le informazioni del traffico telefonico e telematico per l'ipotesi in cui queste si rivelino necessarie alle autorità di pubblica sicurezza è da considerarsi obbligato a procedere – secondo il modello dell'*accountability*[41] – a valutare i rischi del trattamento che pone in essere e ad implementare, di conseguenza, le misure tecniche e organizzative "per garantire un livello di sicurezza adeguato al rischio"[42]. Nonostante, infatti, le regole generali e i principi che concorrono a definire l'*accountability* trovino espressa enunciazione in alcune norme del GDPR, quali gli artt. 5, par. 2, 24 e 32, le "misure tecniche e organizzative" non possono prescindere da un intervento diretto del titolare, che dovrà riempirle di contenuto all'esito di una attività di analisi e di gestione del rischio declinata nella prospettiva del singolo trattamento, anche di quello che risponde a finalità di sicurezza pubblica[43].

Fra le misure tecniche ed organizzative che il titolare del trattamento può mettere in atto pare assumere particolare rilievo quella della pseudonimizzazione[44]. Il trattamento di dati personali con modalità che non consentano il loro collegamento ad una determinata persona fisica senza l'impiego di informazioni aggiuntive, conservate separatamente, identifica senz'altro una delle misure tecniche e organizzative intese a garantire che la conservazione dei dati avvenga nel rispetto di standard adeguati di protezione.

L'indiscutibile vantaggio di una simile misura consiste sicuramente nella sua reversibilità. Il collegamento tra l'informazione e la persona fisica viene meno, mediante la rimozione di qualsiasi riferimento diretto del dato al soggetto interessato, ma al contempo rimane possibile – allorquando si riveli necessaria – la possibilità di una sua re-identificazione, per il tramite di una "chiave" in grado di ricollegare il dato alla persona fisica.

Ciò si rivela, allora, nella prospettiva delle investigazioni digitali, di essenziale importanza, e al contempo pare soddisfare – anche nel contesto di questa indagine – il principio di limitazione della conservazione[45], per effetto del quale la restrizione temporale del trattamento non interviene sul periodo di conservazione delle informazioni in sé; piuttosto, ciò che il legislatore eurounitario ha inteso circoscrivere entro limiti temporali precisi è la relazione tra i dati e la persona fisica a cui essi sono riferiti e che ne consentono l'identificazione o l'identificabilità.

Ruolo di non secondaria importanza è anche quello svolto da altri strumenti di *accountability*, quali quelli che rispondono ai concetti di *data protection* (o *privacy*) *by design* e *by*

41. Il principio di *accountability* promuove un vero e proprio modello nella adozione di standard di sicurezza. Questo, semplicisticamente tradotto nella versione italiana del Regolamento con il termine "responsabilizzazione", indentifica invero un più ampio concetto che evoca anche la responsabilità del titolare del trattamento di assicurare la conformità di questo al GDPR, ciò che si traduce in una sua responsabilizzazione circa l'adozione di adeguati strumenti che la possano realizzare, e a cui si aggiunge, da ultimo, anche la disponibilità della prova di tale conformità. Sul principio di *accountability* v. almeno Gatti 2025, p. 876 ss.; Albanese–Cardinali 2023, p. 501 ss.; Carleo 2021, p. 359 ss.; Amore 2020, p. 414 ss.; Finocchiaro 2019, p. 2778 ss. e Lucchini Guastalla 2018, p. 106 ss.
42. Cfr. art. 32 GDPR.
43. Tale intervento diretto del titolare del trattamento, peraltro, non si esaurisce con l'adozione, ma trova estensione anche ai successivi interventi del riesame e dell'aggiornamento, ove necessario, delle misure introdotte. Cfr., per esempio, Gatti 2025, p. 881 ss.
44. Cfr. art. 4, par. 1, n. 7, GDPR. In commento v., tra gli altri, Almada–Maranhao–Sartor 2023, p. 162 ss. Sul punto v. anche il considerando n. 28 del GDPR, ove si chiarisce che "l'applicazione della pseudonimizzazione ai dati personali può ridurre i rischi per gli interessati e aiutare i titolari del trattamento e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati".
45. Cfr. art. 5, par. 1, lett. e), GDPR. Sul principio di limitazione della conservazione v., per esempio, Roßnagel–Richter 2023, p. 285 ss.

default[46]. In assenza di un criterio temporale che sia a sufficienza ristretto da poter garantire buoni livelli di sicurezza, le modalità di progettazione dei mezzi impiegati nella conservazione e le impostazioni predefinite degli stessi potrebbero, nel concreto, consentire di applicare quelle misure di conservazione targhettizzata che impiegano criteri geografici, ovvero quelli basati sulle persone in qualche misura vicine ad ambienti criminosi, per filtrare i soli dati che potranno potenzialmente risultare rilevanti per le finalità di prevenzione, indagine, accertamento e perseguimento di reati, con l'esito di far così rientrare il trattamento in questione entro i confini della conformità al principio di minimizzazione[47], e di proporzionalità[48].

Criticità decisamente minori sembra, da ultimo, sollevare il trattamento condotto dall'autorità giudiziaria che consiste nella acquisizione dei dati rilevanti per le finalità che le sono proprie, il quale è da far rientrare – come anticipato – nell'ambito di applicazione della direttiva LED. L'accesso, che è ammesso se sussistono sufficienti indizi di reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, è limitato a tali ipotesi specifiche (individuate dallo stesso legislatore) e, sebbene tale limitazione non sia così rigorosa, escludendo – di fatto – tali categorie i soli reati di lieve entità, essa potrebbe in una qualche misura trovare giustificazione – quantomeno dal punto di vista della protezione dei dati personali – nelle lievemente meno stringenti previsioni di tutela della direttiva in tale ambito, che legittimamente comprime la protezione delle informazioni dei soggetti interessati, e i loro diritti, in favore di esigenze di natura pubblicistica, come ammesso anche dallo stesso GDPR, all'art. 23.

Qualche dubbio invece residua sulla compatibilità di tale secondo trattamento con il principio della proporzionalità, poiché troppo ampio pare essere lo spazio operativo (lasciato aperto dalla ampia nozione di "reato grave") delle esigenze di pubblica sicurezza, a discapito di una eccessiva compressione della riservatezza degli utenti. Anche qui, però, vale la pena considerare l'idea che la proporzionalità possa essere ripristinata per il tramite dell'adozione dei già richiamati strumenti di *accountability* che, *ex ante*, innalzano il livello di sicurezza dei dati personali sin dalla fase della loro conservazione.

5. Qualche osservazione conclusiva

Emerge, in definitiva, con la massima evidenza come nel settore delle investigazioni digitali – per quanto qui più rileva, nell'applicazione di misure di *data retention* – la dimensione pubblicistica, che, come detto, prende forma nell'acquisizione di dati che risultano rilevanti ai fini di prevenzione, indagine, accertamento e repressione di reati, abbisogni della cooperazione di soggetti privati, i fornitori di servizi di comunicazione elettronica (titolari del trattamento) che, pur agendo in applicazione di regole di natura privatistica, conservino tali dati e, al contempo, assicurino che l'accesso abbia luogo entro limiti adeguati di sicurezza e integrità delle informazioni.

Tali soggetti – anche in questo specifico ambito – risultano oltremodo "responsabilizzati", perché la mancata, scorretta o inidonea implementazione di misure di sicurezza volte a contenere il rischio specifico li espone ad interventi correttivi da parte dell'Autorità garante o, eventualmente, all'applicazione di sanzioni amministrative. Ma non solo. Per il caso di violazione del Regolamento viene in rilievo, sul piano del *private enforcement*, anche il profilo risarcitorio. Se, infatti, il *provider*, titolare del trattamento, soggetto a precisi ed eccezionali obblighi di ultra-conservazione delle informazioni motivati da interessi di natura pubblicistica, abbia mancato di adottare misure tecniche ed organizzative, o se queste, ancor più essenziali nella situazione in cui il diritto alla protezione dei dati personali regredisce per lasciare spazio ad altre e parimenti rilevanti esigenze di lotta alla criminalità, dovessero, sulla base di una valutazione del caso concreto, rivelarsi

46. Essenziale rimane altresì, ai fini della determinazione – a monte – del livello di rischio, la valutazione di impatto del trattamento previsto sulla protezione dei dati personali.
47. Indubbio è infatti il rapporto di strumentalità delle misure intese ad inverare i concetti di *data protection by design* e *data protection by default* rispetto al principio di minimizzazione. Sul punto v., per esempio, Voigt–von dem Bussche 2024, p. 63 ss. e 138 s.
48. Perché, come osservato dalla stessa Corte di giustizia, misure di tale sorta sarebbero ideonee a garantire un più equo bilanciamento dei diritti e interessi in conflitto.

inadeguate, sarà ritenuto responsabile del danno in ipotesi subito dai soggetti interessati coinvolti[49].

Peraltro, non si può non notare come, così configurati, gli operatori privati vengano a rivestire un ruolo non secondario anche quali fattori correttivi di una disciplina che, specialmente nella determinazione dei periodi di conservazione dei dati del traffico telefonico e telematico, non sembra porsi perfettamente in linea né con il diritto della protezione dei dati personali né con il principio eurounitario della proporzionalità. È solo grazie alle misure di *accountability* introdotte dal *provider* e agli strumenti di sicurezza che questi attua in applicazione di tale modello che la conservazione generalizzata e indifferenziata può essere in una qualche misura temperata, riportando così il trattamento entro i confini di liceità e parimenti scongiurando una – ancorché parziale – disapplicazione dell'art. 132 del Codice in materia di protezione dei dati personali per il suo contrasto con il diritto eurounitario.

Al fine di non aggravare – anche in termini di costi – la posizione già di per sé onerosa, in termini di "responsabilizzazione" del titolare del trattamento, sarebbe, allora, auspicabile un intervento organico e aggiornato da parte del legislatore eurounitario[50]. Gli strumenti normativi del diritto dell'Unione, specie se adottati nella forma del regolamento, si rivelano infatti maggiormente idonei a raccogliere le elaborazioni della Corte di giustizia in un unico *corpus* normativo, a cui gli Stati membri siano chiamati ad adeguarsi senza apprezzabili margini di discrezionalità, nella consapevolezza che solo una disciplina uniforme, direttamente applicabile nei diversi contesti nazionali, può realizzare il necessario contemperamento, conforme agli standard (anche di sicurezza) europei, tra le esigenze pubblicistiche, da un lato, e la tutela dei diritti alla riservatezza e alla protezione dei dati personali dei singoli individui, dall'altro[51].

Riferimenti bibliografici

F. Albanese, I. Cardinali (2023), *Il principio di responsabilizzazione (accountability)*, in F. Bravo (a cura di), "Dati personali. Protezione, libera circolazione e governance, 1. Principi", Pacini Giuridica, 2023

M. Almada, J. Maranhao, G. Sartor (2023), *sub Art. 4(5)*, in I. Spiecker gen. Döhmann, V. Papakonstantinou, G. Hornung, P. De Hert (Eds.), "General Data Protection Regulation. Article-by-Article Commentary", Beck-Hart-Nomos, 2023

G. Amore (2020), *Fairness, Transparency e Accountability nella protezione dei dati personali*, in "Studium iuris", 2020, n. 4

S.G. Battistini, L. Matarazzo, L. Zanetti (2023), *Il principio di minimizzazione dei dati*, in F. Bravo (a cura di), "Dati personali. Protezione, libera circolazione e governance, 1. Principi", Pacini Giuridica, 2023

49. Cfr. art. 82 GDPR. Così ragionando, peraltro, viene messa in luce la stretta connessione tra *accountability* e responsabilità, tale per cui le misure di sicurezza discrezionalmente adottate dal titolare del trattamento divengono parametro di valutazione del rispetto della normativa. Sul punto v. almeno Gatti 2025, p. 893 ss. L'art. 82, letto in connessione all'approccio dell'*accountability*, pare allora avvalorare la conclusione della Corte di giustizia, che qualifica la responsabilità del Regolamento come una responsabilità per colpa, con inversione dell'onere della prova (cfr. Corte giust. Ue, 21 dicembre 2023, C-667/21).
50. In senso conforme v. Flor–Marcolini 2022, p. 119, i quali suggeriscono un intervento legislativo, a livello eurounitario e/o nazionale, che individui i termini della cooperazione (o *co-regulation*) tra settore pubblico e privato nella prevenzione, nell'indagine, nell'accertamento e nel perseguimento dei reati.
51. Se poi si considera che l'obbligo di conservazione dei dati relativi alle comunicazioni elettroniche, da cui discende la possibilità per le autorità di contrasto di avere a questi accesso, è strumento di essenziale importanza per l'accertamento e la repressione delle più diverse forme di criminalità, anche e soprattutto quando la loro esecuzione si estende oltre i confini nazionali, ancor meglio si comprende l'esigenza che la disciplina di riferimento sia inquadrata nel contesto normativo eurounitario, così da garantire un più elevato livello di cooperazione – anche giudiziaria – in materia penale.

R. Carleo (2021), *Il principio di accountability nel GDPR. Dalla regola alla auto-regolazione*, in "Nuovo diritto civile", 2021, n. 1

C.M. Cascione (2014), *I diritti fondamentali prevalgono sull'interesse alla sicurezza: la decisione data retention della Corte di giustizia e gli echi del datagate*, in "Nuova giurisprudenza civile commentata", 2014, n. 11

C. Colapietro, A. Iannuzzi (2017), *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. Califano, C. Colapietro (a cura di), "Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel regolamento UE 2016/679", Editoriale Scientifica, 2017

M. Dell'Utri (2019), *Principi generali e condizioni di liceità del trattamento dei dati personali*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), "I dati personali nel diritto europeo", Giappichelli, 2019

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

G. Finocchiaro (2019), *Il principio di accountability*, in "Giurisprudenza italiana", 2019, n. 12

R. Flor, B. Panattoni (2023), *Digital criminal investigation in Italy. The intersection between data protection and cybersecurity*, in "New Journal of European Criminal Law", vol. 14, 2023, n. 4

R. Flor, S. Marcolini (2022), *Dalla data retention alle indagini ad alto contenuto tecnologico*, Giappichelli, 2022

R. Flor (2015), *Dalla 'Data retention' al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della corte di giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive 'de iure condendo'*, in G. Resta, V. Zeno-Zencovich (a cura di), "Il diritto all'oblio su internet dopo la sentenza Google Spain", Roma TrE-Press, 2015

R. Flor (2014), *La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in "Diritto penale contemporaneo", 2014, n. 2

S. Gatti (2025), *Il principio di accountability e la sua attuazione nel regolamento generale sulla protezione dei dati*, in R. Bocchini (a cura di), "Trattato Le piattaforme digitali. e-Agorà", Giappichelli, 2025

E. Grillo (2024), *Sulla conservazione sistematica e generalizzata di dati genetici e biometrici per finalità di polizia*, in "Nuova giurisprudenza civile commentata", 2024, n. 4

M. Landolfi (2021), *La Corte di Giustizia UE interviene ancora sulla conservazione e sull'accesso ai dati di traffico e di ubicazione: alcune riflessioni sulla disciplina interna*, in "Studium iuris", 2021, n. 12

E. Lucchini Guastalla (2018), *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in "Contratto e impresa", 2018, n. 1

A. Roßnagel, P. Richter (2023), *sub Art. 5,* in I. Spiecker gen. Döhmann, V. Papakonstantinou, G. Hornung, P. De Hert (Eds.), "General Data Protection Regulation. Article-by-Article Commentary", Beck-Hart-Nomos, 2023

L. Trucco (2014), *Data retention: la Corte di giustizia si appella alla Carta UE dei diritti fondamentali*, in "Giurisprudenza italiana", 2014, n. 8-9

P. Voigt, A. von dem Bussche (2024), *The EU General Data Protection Regulation (GDPR). A practical Guide*, 2nd ed., Springer, 2024