DIPARTIMENTO DI GIURISPRUDENZA

Cattedra di Diritto Penale, Parte Speciale

"DATA RETENTION": TRA ESIGENZE DI PUBBLICA SICUREZZA E TUTELA DEI DIRITTI FONDAMENTALI DELLA PERSONA

RELATORE
Chiar.mo Prof.
Maurizio Bellacosa

CANDIDATA
Federica Pittau
Matr. 143063

CORRELATORE
Chiar.ma Prof.ssa
Francesca Minerva

ANNO ACCADEMICO 2020-2021

«Qui custodiet ipsos custodes?»

«Ma chi sorveglierà i sorveglianti stessi?»
(Giovenale, *Satire*, VI, 346-347)

INDICE SOMMARIO

CAPITOLO II

I DIRITTI FONDAMENTALI COINVOLTI DALLA DISCIPLINA DELLA CONSERVAZIONE DEI DATI DI TRAFFICO: TRA PARADIGMI COSTITUZIONALI E CARTE EUROPEE DEI DIRITTI

CAPITOLO III

PROFILI DI CRITICITÀ DELLA DISCIPLINA ITALIANA IN MATERIA DI *DATA RETENTION*

SEZIONE I

Distonie tra l'art. 132 del Codice *Privacy* e il diritto Ue

SEZIONE II

***"Data retention"* e processo penale**

INTRODUZIONE

Negli ultimi decenni, la rete globale e le opportunità offerte dalle nuove tecnologie hanno comportato una costante pressione verso il rinnovamento in tutti gli ambiti fondativi della vita economica e interpersonale, determinando il passaggio dalla società industriale a quella che, secondo la *communis opinio*, viene definita società dell'informazione o informazionale[1]. Con tale espressione, si fa riferimento ad un contesto post-industriale caratterizzato dall'utilizzo pervasivo di tecnologie dell'informazione e della comunicazione (in acronimo *TIC* o *ICT*, dall'inglese *information* and *communications technology*), cioè da strumenti e tecniche impiegate nella trasmissione, ricezione ed elaborazione di dati e informazioni (tecnologie digitali comprese). A ben ragione si parla di "Rivoluzione informatica"[2] o di "Terza Rivoluzione industriale" in quanto lo spasmodico utilizzo delle *TIC* ha comportato non solo l'ampliamento del novero – già di per sé consistente – dei mezzi comunicazione, rendendoli tendenzialmente accessibili a chiunque in qualsiasi momento, ma ha investito ogni sfera della vita privata e collettiva.

Nel campo del diritto penale, angolo visuale del presente lavoro, i moderni mezzi dell'informatica hanno determinato l'insorgenza di nuove forme di criminalità, c.d. *cybercrimes*[3], ma, soprattutto, hanno fornito agli organi investigativi sofisticati e penetranti strumenti di ricerca e di raccolta prove, sempre più invasivi. In tal senso, assume un rilievo fondamentale sul terreno dell'accertamento dei reati il ricorso generalizzato agli strumenti di raccolta di dati personali (siano essi dati relativi ad

[1] L'espressione utilizzata nel testo è stata coniata da CASTELLS, *The information age: economy, Society and Culture*, Oxford, 2010. Nella celebre trilogia sopracitata, l'Autore inglese ha osservato che la società dell'informazione costituisce un nuovo paradigma socio-tecnologico in cui il tradizionale scambio tra chi produce merci e chi fornisce materie prime è stato sostituito dallo scambio tra chi produce conoscenza tramite l'elaborazione di informazioni e chi fornisce il lavoro necessario per attivare processi produttivi basati su quella conoscenza. In questo contesto socio-tecnologico, è considerata "risorsa strategica" prevalente la manipolazione di informazioni e il valore economico della conoscenza. Alla "produzione di merci a mezzo di merci" è subentrata la "produzione di informazione a mezzo di informazione" in contesto transattivo completamente dematerializzato e caratterizzato da una serie di aspetti: la pervasività, la flessibilità, la convergenza e l'interconnessione.

[2] Cfr. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione – Corso di informatica giuridica*, Torino, 2016, 3.

[3] Per un approfondimento sulla nozione di "cybercrime" si rinvia a LORUSSO, "Digital evidence", "cybercrime" *e giustizia penale 2.0*, in *Processo penale e Giustizia*, 2019, 821.

immagini, dati digitali, dati "non comunicativi"[4], nonché, dati "esterni" alla conversazione)[5]. In siffatta categoria, soggetta ad ampliamento costante, rientra l'attività di conservazione e di acquisizione, presso i fornitori dei servizi di comunicazione, dei dati relativi al traffico telefonico e telematico, c.d. *data retention*.

L'istituto *de quo*, caratterizzato da una genesi e un'evoluzione normativa complessa[6], ha ad oggetto tutte le tracce relative ad operazioni comunicative già avvenute, mediante telefono cellulare o rete *Internet*. È, infatti, ormai indiscussa la "potenzialità euristica"[7] di siffatte informazioni le quali, pur prescindendo dal contenuto della conversazione, sono in grado di rilevare la coordinate spaziali e temporali dell'utenza mobile – e, in via mediata, del suo detentore – nonché i contatti telefonici e telematici da quest'ultimo prestabiliti[8]. Per assicurarne la disponibilità a fini di indagine, i gestori dei servizi informatici e telematici risultano destinatari di un vero e proprio obbligo *ex lege,* secondo cui è imposta l'archiviazione dei dati di cui trattasi per un periodo di tempo prestabilito. Durante tale lasso di tempo, gli organi inquirenti hanno la possibilità di accedere a siffatte informazioni, contenute in tabulati telefonici in forma cartacea o digitale, e disporne l'acquisizione all'interno del procedimento penale.

Negli ultimi anni, la metodologia di indagine di cui trattasi è stata al centro di un ampio dibattito giurisprudenziale e dottrinale che, travalicando i confini della sovranità nazionale, ha raggiunto il suo *akmè* in ambito comunitario. La *vexata questio* si riassume efficacemente attraverso le due espressioni evocate nel titolo del presente lavoro: pubblica sicurezza (*auctoritas*) e diritti fondamentali della persona (*libertas*)[9]. Con la locuzione "pubblica sicurezza" si fa riferimento ad un concetto che, nella sua accezione generica, ricomprende l'interesse collettivo alla repressione nei reati, dotato

[4] La differenza tra dati "comunicativi" e "non comunicativi" è stata evidenziata da SIGNORATO, *Novità in tema di* data retention*. La riformulazione dell'art. 132 codice privacy da parte del D. Lgs. 10 agosto 2018 n. 101*, in *Dir. Pen. contemp.*, 2018, 153. Il punto sarà oggetto di trattazione nel Cap. I.
[5] Così ANDOLINA, *L'ammissibilità degli strumenti di captazione dei dati personali tra standard di tutela della* privacy *e onde eversive*, in *Arch. pen.*, 2015, n. 3, 916.
[6] Per un approfondimento sul punto, si rinvia al Cap. I.
[7] L'espressione è CONTI, *Sicurezza e riservatezza, in Dir. pen e proc,* 2019, 1572.
[8] Cfr. Cap I § 4.1.
[9] V. ORLANDI, *La riforma del processo penale fra correzioni strutturali e tutela progressiva dei diritti fondamentali*, in *Rivista italiana di diritto e procedura penale*, 2014, 1151. L'Autore sottolinea l'esigenza di ridefinire, in ambito processuale, il baricentro tra *auctoritas* e *libertas,* salvaguardando contemporaneamente il nucleo duro dei diritti fondamentali e l'esigenza di pubblica sigurezza.

di fondamento costituzionale grazie al combinato disposto tra gli artt. 2 e 112 Cost[10]. Il secondo termine del conflitto, invece, fa riferimento ad un ampio agglomerato di situazioni giuridiche soggettive espressamente riconosciute dalla Costituzione e dalle Carte dei diritti fondamentali[11].

L'esigenza di ridefinire continuamente il baricentro tra siffatti valori, ontologicamente in contrasto tra di loro, spiega la difficoltà del legislatore nell'individuare i limiti che circoscrivano l'ambito di applicazione della c.d. *data retention*. Se da una parte è indubbio che la conservazione dei dati di traffico telefonico e telematico possa rivelarsi uno strumento prezioso per l'accertamento dei reati, dall' altra, risulta altrettanto evidente che la loro acquisizione all'interno del procedimento penale realizzi una vistosa ingerenza nei confronti della riservatezza, sia intesa come tradizionale "libertà negativa"[12], sia nella sua accezione più ampia e comprensiva di forme di tutela innovative.

Ciò posto, questo studio nasce dalla volontà di analizzare come la costante oscillazione tra le esigenze contrapposte di cui *supra* abbia delineato una parabola evolutiva in tema di *data retention*, volta a privilegiare, in modo graduale, la tutela dei diritti inviolabili dell'individuo rispetto alla logica di prevenzione e di repressione dei reati. Siffatto *iter*, ancora in atto, è stato, però, contrassegnato da continue contraddizioni tra legislatore e giurisprudenza nazionale e europea che hanno dato spesso luogo a soluzioni contrastanti in materia di conservazione e acquisizione dei dati "esterni" alla comunicazione. Il presente lavoro ripercorrerà le tappe fondamentali che hanno condotto all'assetto normativo attuale e le prospettive *de iure condendo,* ispirate dalle coordinate segnate dai principi di proporzione e legalità di provenienza comunitaria.

A tal proposito, si verificherà come, il legislatore italiano abbia, fin da subito, incontrato difficoltà nell'inquadrare l'istituto della *data retention* come fenomeno giuridico di natura processualpenalistica, riservando ad esso una insolita collocazione *extra-codicem*. Inoltre, mediante la ricostruzione della lunga evoluzione normativa, si avrà modo di constatare come, nell'ordinamento interno, si siano privilegiate esigenze di contrasto alla criminalità organizzata e al terrorismo internazionale, a discapito della

[10] Cfr. Cap I §1.
[11] Cfr. Cap II.
[12] Sul punto si veda SILVESTRI, *L'individuazione dei diritti della persona*, in *Dir. pen. Cont.*, 2018, 1.

tutela dei diritti fondamentali. Non è, infatti, un caso che le più importanti modifiche in materia di conservazione dei dati di traffico siano state predisposte a seguito di attentati terroristici sul territorio europeo[13]. Siffatta tendenza del legislatore nostrano verrà, poi, confermata dall'ultima modifica del Codice *Privacy* che, mediante l'introduzione di una norma di natura derogatoria, realizza una grave sacrificio della "sfera privata" dell'individuo[14].

Inoltre, si evidenzierà come, in contrapposizione all'approccio "securitario" del legislatore nazionale, si sia riscontrato un atteggiamento maggiormente "garantista" della Corte di Giustizia dell'Unione Europea, a cui è da attribuire il merito di aver individuato con chiarezza i diritti fondamentali aggrediti dalla c.d. *data retention*. Si vedrà come, a partire dalla storica sentenza *Digital Ireland e Seitlinger*[15] fino alla recentissima pronuncia *H.K. Danmark*[16]*,* i giudici di Lussemburgo abbiano rimodulato il binomio sicurezza-tutela dei diritti mediante l'individuazione di elevati *standard* che, in piena conformità alla cornice dei valori coinvolti, rispondano al principio di proporzionalità. Mediante l'analisi di siffatti rilievi, si darà conto dell'avvio di un processo di revisione critica avente ad oggetto non solo la disciplina comunitaria ma anche gli assetti normativi nazionali in materia di conservazione dei dati di traffico.

Gettando poi uno sguardo sugli approdi interpretativi della giurisprudenza nazionale, si segnalerà l'atteggiamento di "resistenza"[17] che il legislatore e la magistratura hanno sinora riservato alle novità provenienti dall'Unione europea[18]. Un dibattito tutt'ora in corso e che sembra destinato a svilupparsi ulteriormente, nella perpetua ricerca di un punto di equilibrio tra le esigenze di tutela della pubblica sicurezza e dei diritti fondamentali della persona. Infine, evidenziando le criticità e i vuoti di tutela dell'assetto normativo attuale si delineeranno, in un'ottica *de iure*

[13] Cfr. Cap I § 3.6.
[14] Cfr. Cap I § 4.4.
[15] Si fa riferimento alla Corte giust. UE, Gr. Sez., sent. 8 aprile 2014, *Digital Rights*, che sarà oggetto di un'ampia disamina nel Cap. § 9.
[16] Si fa riferimento Corte giust. UE, Gr. Sez., sent. 2 marzo 2021, *H.K. Danmark,* approfondita nel Cap II § 11.
[17] L'espressione è di LUPÀRIA, Data retention *e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, in *Dir. internet,* 2019, 4, 760.
[18] Il punto verrà approfondito nel Cap. III § 4.

condendo, le coordinate sostanziali e processuali[19] di una possibile riforma da parte del legislatore nazionale in tema di *data retention*.

[19] Cfr. Cap III §5.

CAPITOLO I

INQUADRAMENTO DELLA DISCIPLINA DELLA C.D. *DATA RETENTION* NELL'ASSETTO NORMATIVO NAZIONALE E EUROPEO

1. Linee generali dell'istituto.

Ogni qualvolta si effettui una conversazione tramite "rete telefonica o telematica"[20], sono generate una serie di informazioni relative all'utente che vengono archiviate automaticamente dal gestore del servizio prescelto[21]. Tra di esse, si annoverano, a titolo meramente esemplificativo, il numero del mittente e del destinatario della chiamata, l'ora e la sua durata e le celle telefoniche agganciate durante la conversazione[22]. Tali dati sono definiti "esterni" in quanto sono caratterizzati da un'intrinseca estraneità rispetto al contenuto della comunicazione di cui precludono la conoscibilità. Mediante gli stessi si è invece in grado apprendere le coordinate spaziali e temporali dell'utenza "mobile"[23], e in via mediata del suo detentore, in un preciso momento e dei contatti telefonici o telematici che questi abbia avuto nel medesimo lasso di tempo[24]. Il rilievo investigativo delle informazioni

[20]Con "rete telefonica o telematica" si fa riferimento ad un articolato sistema di linee elettriche che consentono la predisposizione di servizi di comunicazione. Tali apparati rientrano nella più ampia categoria delle «reti di comunicazione elettronica» di cui l'art. 2, lett. *a)* della direttiva quadro 2002/21/CE offre puntuale definizione. Si tratta di «sistemi di trasmissione» e di «apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse (a commutazione di circuito e a commutazione di pacchetto, compresa Internet), le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato».

[21] Si veda MARCOLINI, *L'istituto della* data retention *dopo la sentenza della corte di giustizia del 2014* in AA. VV., *Cybercrime,* (a cura di) CADOPPI, CANESTRARI, MANNA, PAPA, Torino, 2019, 1580.

[22] Per un maggiore approfondimento sul punto *infra,* Cap. I § 4.1.

[23] Con tale espressione si fa riferimento a *computer* e telefoni cellulari che oggigiorno rappresentano, nelle loro varie declinazioni (*netbook*, *tablet*, *smartphone*), la principale piattaforma attraverso cui le persone gestiscono le proprie relazioni sociali, sia di tipo lavorativo sia di natura privata e personale. In particolar modo, la telefonia cellulare è una modalità di accesso ad una rete telefonica realizzata per mezzo di onde radio e ricetrasmettitori terrestri. Tale sistema di comunicazione *wireless*, o senza fili, colloca in grandi aree geografiche settori più piccoli chiamate "celle", da cui deriva il termine "cellulare". La divisione in celle permette di utilizzare la stessa frequenza per celle distanti tra loro, senza che subentrino interferenze. Cfr. SCACCIANOCE, *Approvvigionamento di flussi e dati tramite il dispositivo telefonico altrui,* in AA. VV., *Le indagini atipiche,* SCALFATI (a cura di), Torino, 2014, 29.

[24] Cfr. Cap. I § 4.1.

suddette è facilmente intuibile in quanto consente alle autorità inquirenti di testare la veridicità delle tesi difensive prospettate dall'imputato o dalla persona offesa[25].

La disciplina avente ad oggetto l'attività di conservazione e di acquisizione dei dati "esterni" alle comunicazioni per finalità accertamento e repressione dei reati è conosciuta con il termine "data retention*"*.

In un primo tempo, l'istituto si è imposto come fenomeno tecnologico prima ancora che giuridico[26] riscontrandosi una diacronìa[27] tra il momento dell'emersione nella prassi investigativa, e quello della sua regolamentazione normativa. Come frequentemente accade per le metodologie investigative di carattere tecnologico-scientifico, tale strumento è stato, dunque, piegato alle esigenze di indagine, nella totale indifferenza del legislatore.

Sul lento e faticoso conio dell'istituto come fenomeno giuridico hanno indubbiamente pesato la difficoltà di pervenire all'individuazione del bene giuridico sul quale incide l'acquisizione dei dati di traffico[28]. L'evoluzione del quadro normativo costituisce uno strumento rivelatore del processo di progressiva messa a fuoco di tale elemento e testimonia il diverso atteggiarsi di interessi contrapposti nel corso del tempo. La loro reciproca influenza ha portato ad una costante oscillazione tra *auctoritas* e *libertas*[29]*,* tra istanze di repressione dei reati e esigenze di tutela delle libertà fondamentali.

---

[25] A riprova di siffatta rilevanza investigativa si vedano i casi di cronaca in cui la tesi difensiva prospettata dall'indagato viene smentita o confermata dall'uso di un *computer* in una certa fascia oraria, o dalla localizzazione dell'indagato in un certo momento mediante l'acquisizione dei tabulati telefonici. *Inter alios*, si fa riferimento al caso di Garlasco (su cui v. COLOMBO, *La sentenza del caso di Garlasco e la* computer forensics*: analisi di un complesso rapporto tra diritto e informatica*, in *Cyberspazio e diritto*, 2010, 277) e al c.d. stupro della Caffarella di Roma, in cui i due indagati sono stati scagionati dal *test* del DNA e dalla ricostruzione del traffico telefonico, Nel caso di specie, le utenze mobili dei due uomini non risultavano agganciate alle celle telefoniche presenti nella zona della Caffarella durante il *tempus commissi delicti*. Sul punto, si veda DI PAOLO, *La prova informatica*, in *Enc. Dir.*, 2013, *nota* 11.

[26] In tal senso, RUGGIERI, *Divieti probatori e inutilizzabilità nella disciplina delle intercettazioni telefoniche*, Milano, 2001, 84.

[27] L'espressione è di ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, Milano, 2018, XII.

[28] Sul punto CONTI, *L'attuazione della direttiva Frattini: un bilanciamento insoddisfacente tra riservatezza e diritto alla prova*, in AA. VV., *Le nuove forme sulla sicurezza pubblica*, LORUSSO (a cura di), Padova, 2008, 7.

[29] V. ORLANDI, *La riforma del processo penale fra correzioni strutturali e tutela progressiva dei diritti fondamentali*, in *Rivista italiana di diritto e procedura penale*, 2014, 1151. L'autore sottolinea l'esigenza di ridefinire continuamente il baricentro tra *auctoritas* e *libertas,* salvaguardando contemporaneamente il nucleo duro dei diritti fondamentali. Rimarca inoltre l'esigenza di salvaguardare il «confine mobile che – sulla scorta di valutazioni e bilanciamenti mutevoli nel tempo- divide l'area

La disciplina attualmente vigente in materia di *data retention* affonda le proprie radici nel tortuoso cammino che la giurisprudenza ha compiuto al fine di individuare il corretto bilanciamento tra le due esigenze contrapposte, sopperendo all'assenza di una normativa *ad hoc.* L'esegesi delle prassi applicative di origine pretoria costituisce, dunque, elemento imprescindibile per comprendere appieno l'assetto normativo attuale in materia.

2. L'approccio giurisprudenziale ai tabulati telefonici: un dialogo tra le Corti.

La Corte costituzionale si è occupata per la prima volta dell'acquisizione dei tabulati telefonici nel 1993[30] con una storica pronuncia ancora oggi fondamentale per l'attualità dei principi enunciati[31]. Nel caso *de quo*, il giudice delle leggi era chiamato ad esprimersi sulla questione di legittimità costituzionale[32] della disciplina delle intercettazioni (artt. 266 c.p.p. e ss.) nella parte in cui non prevedeva l'estensione delle garanzie processuali anche all'attività di acquisizione dei tabulati di traffico telefonico. Nell'ordinanza di remissione, il pretore constatava che la giurisprudenza prevalente fosse concorde nell'identificare le intercettazioni come mezzo di captazione del

dei diritti individuali da quella di una loro compressione giustificata dalla necessità di reprimere e/o prevenire attività criminose».

[30] Si fa riferimento alla sentenza Corte cost., 11.03.1993, n. 81, in *www.cortecostituzionale.it.* Sul contenuto della sentenza v. DI FILIPPI, *Dati esteriori delle comunicazioni e garanzie costituzionali*, in *Giur. It.*, 1995, fasc. 1, 117; PACE, *Nuove frontiere della libertà di "comunicare riservatamente" (o, piuttosto, del diritto alla riservatezza)?*, *ivi*, 1993, 742; POTETTI, *Corte costituzionale n. 81/93: la forza espansiva della tutela accordata dall'art. 15 comma 1 Cost.*, in *Cass. Pen*., 1993, 2746.

[31] In tale senso RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico. - Il bilanciamento tra privacy e repressione del fenomeno criminale nel dialogo tra giurisprudenza e legislatore*, in *Dir. Pen. contemp*., 2016, 3, 158.

[32] Pret. Macerata, ord. 8 aprile 1992, in *Arch. n. proc. pen.*, 1992, 512. La *quaestio legitimitatis* era stata sollevata nel corso di un giudizio instaurato a seguito dell'opposizione al decreto penale con cui si accusava l'imputata del reato di molestia o di disturbo alle persone commesso per mezzo del telefono ai sensi dell'art. 660 c.p. Davanti alla richiesta del pubblico ministero di addurre come prova il tabulato dell'utenza telefonica dell'imputata, la difesa ne aveva eccepito l'inammissibilità sostenendo che questo fosse stato acquisito senza il rispetto delle garanzie previste dagli articoli 266 ss. c.p.p in materia di intercettazioni. Il pretore riconosceva che il formante giurisprudenziale in materia fosse concorde nell'identificare le intercettazioni come mezzo di captazione del contenuto della comunicazione in atto. Riteneva, però, che l'applicazione di tale interpretazione agli artt. 266 c.p.p e ss. fosse in contrasto con il principio di segretezza delle comunicazioni ai sensi dell'art. 15 Cost. Tale discordanza sarebbe stata risolta soltanto attraverso un'operazione ermeneutica volta ad ampliare la nozione di intercettazione in modo tale da comprendere al suo interno l'acquisizione dei dati esterni alle conversazioni e da estendere a questo istituto le garanzie codicistiche previste. Ciò posto, l'autorità remittente sollevava d'ufficio la questione di legittimità costituzionale dell'articolo 266 c.p.p. e richiedeva al Giudice delle leggi una pronuncia additiva.

contenuto della comunicazione in atto[33]. Riteneva, però, che una definizione così circoscritta dell'istituto in esame, non comprensiva dell'acquisizione dei tabulati telefonici, causasse una rimarchevole frizione con il principio di inviolabilità e segretezza della corrispondenza previsto all'art 15 della Costituzione[34]. Tale attività risultava infatti priva di apposita disciplina e finiva per essere realizzata in assenza di opportune garanzie processuali. Ciò era quanto, di fatto, si era verificato nel caso di specie.

In risposta all'eccezione prospettata dal giudice *a quo*, la Corte analizzava tre distinti profili inerenti all'acquisizione dei dati di traffico telefonico, dando un primo inquadramento giuridico alla materia[35].

Innanzitutto, ribadiva l'adesione all'interpretazione restrittiva dell'istituto delle intercettazioni affermando che la disciplina codicistica si riferisse «esclusivamente a operazioni relative al contenuto di conversazioni (telefoniche)». A sostegno di tale approccio ermeneutico, adduceva la constatazione di una differenza ontologica e strutturale tra gli istituti presi in esame. Da un lato, le intercettazioni – secondo una disciplina ancora in vigore – consistono in una tecnica di apprensione[36] del contenuto della comunicazione, nel momento stesso in cui questa viene prodotta. In caso contrario, la conversazione sarebbe inaccessibile se non a coloro che siano parte della conversazione medesima. Dall'altro, la metodologia di indagine relativa ai tabulati telefonici consenti(va) l'acquisizione dei dati "esterni" della comunicazione – e non del suo contenuto – a seguito di una preventiva memorizzazione da parte dei gestori dei servizi. La "dicotomia essenziale"[37] tra i due istituti risiede dunque nella differenza

[33] Sulla definizione di intercettazione si veda *infra.*

[34] Per un approfondimento sulle interferenze tra la c.d. *data retention* e il valore della segretezza delle comunicazioni si rimanda al Cap. II.

[35] Nel caso di specie, la Corte costituzionale si soffermava soltanto sull'attività di acquisizione dei tabulati telefonici e non anche dei dati di traffico telematico. Ciò non deve destare alcuna sorpresa in quanto gli strumenti di comunicazione elettronica all'epoca erano fermi ad uno stato embrionale e avevano raggiunto un raggio di diffusione ridotto, assolutamente non paragonabile a quello attuale. In quegli anni, un interesse della giurisprudenza verso tali flussi informatici sarebbe stato, dunque, inutile oltre che anacronistico. Ciò posto, le osservazioni che seguono sono valide anche per l'attività di apprensione dei tabulati di traffico elettronico e telematico, a cui si farà in seguito riferimento.

[36] Si fa riferimento all'attività di acquisizione da parte dell'autorità giudiziaria. Mediante tale operazione di c.d. *adprehensio* si realizza l'impossessamento dei dati di traffico contenuti nei tabulati telefonici. Sulla differenza tra l'atto di apprensione nella c.d. *data retention* e gli altri mezzi di ricerca della prova si veda *infra*.

[37] L'espressione è di RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico*, *cit.*, 158.

tra l'atto comunicativo in sé e le informazioni esterne attestanti l'identità degli utenti e della loro ubicazione spazio-temporale.

Per le ragioni appena sintetizzate, il Giudice delle leggi si rifiutava di emanare la pronuncia additiva richiesta dal pretore remittente, mediante la quale si sarebbe estesa la disciplina delle intercettazioni ai tabulati telefonici. Tale conclusione, tuttavia, non ha impedito alla Corte di affrontare la questione circa la riconducibilità dell'acquisizione di dati esteriori alle comunicazioni alla garanzia costituzionale prevista dall'articolo 15 Cost. Su tale questione, si è pronunciata in senso affermativo ritenendo che il parametro previsto da tale norma è così ampio «da ricomprendere non soltanto la segretezza del contenuto della comunicazione, ma anche quella relativa all'identità dei soggetti e ai riferimenti di tempo e di luogo della comunicazione stessa»[38]. Si rilevava dunque che l'istituto in esame incide sulla libertà e sulla segretezza della corrispondenza, seppur con minore intensità rispetto alle intercettazioni.

Da tale affermazione, derivava il terzo ed ultimo punto oggetto della pronuncia secondo cui anche riguardo all'attività in esame è necessario rispettare il livello minimo di garanzie processuali dell'articolo 15 Cost[39]. Per evitare di incorrere in una violazione del paradigma costituzionale sopracitato, la Corte individuava una serie di requisiti soggettivi e oggettivi. Si riteneva che l'attività di acquisizione dei dati di traffico potesse essere predisposta laddove fosse emanato un atto proveniente da parte di qualunque autorità giudiziaria, inclusi pubblico ministero, il giudice per le indagini preliminari o il giudice del dibattimento. La riserva di giurisdizione prevista dall'art. 15 Cost. era stata, infatti, sostituita da una più tenue riserva dell'autorità giudiziaria. Per quanto concerne invece l'elemento oggettivo, l'atto di autorizzazione doveva essere adeguatamente motivato al fine di far emergere la sussistenza di esigenze istruttorie finalizzate alla prevenzione e alla repressione dei reati.

[38] In dottrina, nello stesso senso CAMON, *Le intercettazioni nel processo penale*, Milano, 1996, 28. L'Autore evidenzia come le informazioni esterne alla conversazione, essendo dotate di una potenzialità euristica non trascurabile sulla personalità dell'utente, rientrano nella tutela prevista dall'art 15 Cost. al pari delle intercettazioni.

[39] Inoltre, la Corte ha negato che possano validamente ammettersi in giudizio prove assunte in violazione delle garanzie processuali predisposte dall'art. 15 Cost. Per un approfondimento sulla categoria controversa della "prova incostituzionale" si rimanda al Cap. III.

In sintesi, la Corte sorvolava sul requisito di riserva di legge previsto nella sopracitata norma di rango fondamentale, tipizzando una serie di garanzie processuali in attesa dell'intervento del legislatore.

Davanti al *dictum* della Corte costituzionale, la giurisprudenza si è mostrata fortemente disorientata, talvolta aderendo alla soluzione prospettata dal giudice delle leggi, talvolta pronunciandosi con essa in manifesto contrasto[40]. Al fine di dirimere tali discordanze, il Giudice delle leggi è intervenuto nuovamente[41] sul tema dell'acquisizione dei tabulati, riconfermando con forza i principi enunciati nel 1993 e realizzando un formante definitivo in materia.

Nel caso di specie, la Corte era stata chiamata a pronunciarsi sulla legittimità costituzionale dell'articolo 267 comma 1 c.p.p.[42], nella parte in cui richiedeva il provvedimento autorizzativo del giudice per le intercettazioni e non per l'acquisizione dei tabulati telefonici. Secondo il giudice remittente[43], il fatto che entrambe le metodologie di indagine realizzassero una «compressione dell'identico valore della segretezza delle comunicazioni» mal si conciliava con tale disparità normativa, che

---

[40] In particolar modo, è da segnalare il *revirement* realizzato dalla Cassazione a Sezioni Unite con la sentenza del 13 luglio 1998. Nella pronuncia, a seguito di una completa ricognizione della giurisprudenza in materia, si compiva una operazione di equiparazione tra il tabulato telefonico predisposto dall'ente gestore del servizio e il documento redatto dall'autorità giudiziaria al termine dell'intercettazione ex articolo 266-*bis* c.p.p. Introdotta dalla legge 547/1993, tale norma consente l'intercettazione del flusso di comunicazioni relativo a sistemi telematici e informatici, la cui attività viene documentata in forma simile al tabulato. Nonostante l'affinità, è evidente la differenza ontologica tra gli strumenti presi in esame: la documentazione di cui all'art. 266-*bis* c.p.p. si riferisce sempre all'atto comunicativo in sé e non ai dati esterni relativi all'utente. Al contrario, le Sezioni Unite hanno realizzato un vero e proprio accostamento tra gli stessi, stravolgendo i principi espressi nel sopracitato precedente della Corte costituzionale. Soltanto quattro giorni dopo, il Giudice delle leggi è intervenuto nuovamente in materia (vedi *supra*) sconfessando definitivamente tale approccio. Per una lettura completa della sentenza Cass., Sez. Un., 13.07.98, n. 21, in *Cass. pen*., 1999, 465 con nota di MELILLO, *L'acquisizione dei tabulati relativi al traffico telefonico fra i limiti normativi ed equivoci giurisprudenziali*, *ivi*, 473.

[41] Si fa riferimento alla sentenza Corte cost., 17.07.1998, 281, in *www.cortecostituzionale.it*.

[42] L'art. 267 c.p.p. rubricato «Presupposti e forme del provvedimento» delinea l'iter procedimentale da seguire per predisporre un'intercettazione.

[43] Per l'ordinanza di rimessione si veda Trib. Catanzaro, ord. 28 aprile 1997. Nel caso di cui trattasi, il pubblico ministero aveva acquisito durante le indagini preliminari un tabulato telefonico relativo all'utenza cellulare intestata a persona diversa dall'indagato, ma a sua volta imputata in un procedimento connesso. Davanti alla richiesta di ammissione di tale mezzo prova ai sensi dell'art. 493 c.p.p., la difesa ne aveva eccepito l'inutilizzabilità sotto il profilo della carenza di autorizzazione da parte del g.i.p. Il giudice remittente, richiamando incidentalmente la sentenza 11 marzo 1993, n. 81 della Corte costituzionale, riteneva che il decreto acquisitivo del pubblico ministero fosse sufficiente a soddisfare il requisito soggettivo previsto all'art. 15 comma 2 Cost., come riletto nella suddetta pronuncia. Censurava, però, l'articolo 267 comma 1 c.p.p., nella misura in cui realizzava una sperequazione normativa tra l'istituto delle intercettazioni e quella dell'acquisizione dei tabulati telefonici, rimettendo la questione alla Corte costituzionale.

dunque costituiva una vistosa violazione dell'articolo 3 Cost. Per sopperire alla stessa, veniva richiesta una pronuncia additiva che estendesse le garanzie delle intercettazioni all'attività di apprensione dei tabulati.

Posta davanti a tale *quaestio legitimitatis*, il Giudice delle leggi esordiva rimarcando la differenza ontologica tra le due metodologie di indagine e la loro diversa incidenza sul diritto fondamentale enunciato all'articolo 15 Cost. Ciò, di fatto, legittimava la mancata estensione della disciplina delle intercettazioni[44], prevista agli articoli 266 c.p.p. e seguenti. – compreso l'articolo 267 c.p.p. – all'attività di apprensione dei dati esteriori alle conversazioni.

In conclusione, la Corte costituzionale dichiarava la questione di legittimità prospettata dal giudice *a quo* inammissibile, pronunciando una sentenza interpretativa di rigetto. Rimarcava poi la necessità di un solerte intervento legislativo in materia tale da «disciplinare in modo organico l'acquisizione e l'utilizzazione della documentazione relativa al traffico telefonico, in funzione della specialità di questo particolare mezzo di ricerca della prova»[45].

3. L'evoluzione normativa in materia di acquisizione dei dati di traffico: l'incerto cammino del legislatore italiano.

In base a quanto appena illustrato, l'iniziale intervento della giurisprudenza ha avuto come oggetto esclusivo la fase di acquisizione dei tabulati all'interno del procedimento penale. La fase preliminare e ad essa complementare di conservazione dei dati è stata invece al centro del primo intervento da parte del legislatore. Sotto la spinta di istanze di provenienza comunitaria, che hanno trovato piena consacrazione soltanto nel d.lgs. 30 giugno 2003, n. 196 (c.d. Codice *Privacy*)[46], si è provveduto a disciplinare la conservazione dei dati esteriori delle comunicazioni telefoniche con il d.lgs. 13 maggio 1998, n. 171[47].

[44] Sulla disciplina delle intercettazioni si veda Cap I § 5.1.
[45] Sul punto CONTI, *L'attuazione della direttiva Frattini*, *cit.*, 6.
[46] Cfr. Cap I § 3.1.
[47] Recante «Disposizioni in materia di tutela della vita privata nel settore delle telecomunicazioni, in attuazione della direttiva 97/66/CE del Parlamento europeo e del Consiglio, ed in tema di attività giornalistica (modificato dal d.lg. 467/2001)».

Tale decreto costituiva un'appendice della l. 30 dicembre 1996, n. 675 in materia di tutela dei dati personali[48] ed è stato emanato in attuazione della direttiva 1997/66/CE[49]. Ai fini della presente ricerca, è utile svolgere una breve esegesi dell'articolo 4[50] del suddetto decreto, ormai non più in vigore[51]. Al primo comma si enunciava il principio generale secondo cui le informazioni relative al traffico telefonico non potessero essere oggetto di alcun trattamento[52] salvo le deroghe previste nei commi successivi. Dopo aver fornito una puntuale elencazione dei dati ascrivibili a tale categoria, si specificava che l'attività di conservazione, ricompresa nella nozione di trattamento, fosse consentita su consenso dell'interessato e soltanto per il periodo per cui era ammessa la contestazione della fatturazione. Una volta decorso tale

[48] La l. 30 dicembre 1996, n. 675 aveva l'obiettivo di attuare i principi espressi dalla Convenzione di Strasburgo del 1981 («Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale», su cui si è intervenuti nel 2018 con l'adozione del protocollo di modifica detto anche "Convenzione 108+") e dalla direttiva 1995/46/CE (definitivamente abrogata con l'emanazione del c.d. GDPR). Tale strumento legislativo, ha realizzato per la prima volta una disciplina organica e completa in materia di trattamento dei dati personali. Nell'ampia definizione di «trattamento» prevista dall'articolo 1 comma 2 lett. *b)* poteva indubbiamente ricondursi l'attività di archiviazione dei dati di traffico prevista dal d.lgs. 171/1998. Per un approfondimento sul punto si rinvia al Cap II.

[49]Recante «Direttiva 97/66/CE del Parlamento europeo e del Consiglio del 15 dicembre 1997 sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni». Per consultare *online* l'atto normativo ormai abrogato si veda *www.eur-lex.europa.eu.*

[50] Di seguito si riportano integralmente i primi tre commi dell'articolo 4 del d.lgs. 13 maggio 1998, n. 171, rubricato «Dati relativi al traffico e alla fatturazione»:

1. «I dati personali relativi al traffico, trattati per inoltrare chiamate e memorizzati dal fornitore di un servizio di telecomunicazioni accessibile al pubblico o dal fornitore della rete pubblica di telecomunicazioni, sono cancellati o resi anonimi al termine della chiamata, fatte salve le disposizioni dei commi 2 e 3.

2. Il trattamento finalizzato alla fatturazione per l'abbonato, ovvero ai pagamenti tra fornitori di reti in caso di interconnessione, è consentito sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento. Per le medesime finalità, possono essere sottoposti a trattamento i dati concernenti:

a) il numero o l'identificazione della stazione dell'abbonato; b) l'indirizzo dell'abbonato e il tipo di stazione;

c) il numero dell'abbonato chiamato; d) il numero totale degli scatti da considerare nel periodo di fatturazione;

e) il tipo, l'ora di inizio e la durata delle chiamate effettuate e il volume dei dati trasmessi; f) la data della chiamata o dell'utilizzazione del servizio; g) altre informazioni concernenti i pagamenti».

3. Ai fini della commercializzazione di servizi di telecomunicazioni, propri o altrui, il fornitore di un servizio di telecomunicazioni accessibile al pubblico può trattare i dati di cui al comma 2 se l'abbonato ha dato il proprio consenso».

[51] Il decreto legislativo 171/1998 è stato abrogato a partire dal 1.01.2004 *ex* d.lgs. 196/2003.

[52] Ai sensi dell'articolo 1 comma 2 lett. *b)* della l. 30 dicembre 1996, n. 675 con «trattamento» si intendeva «qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati».

periodo, i gestori dei servizi erano tenuti alla cancellazione ai sensi del terzo comma del predetto articolo.

Ne risultava che il gestore dei servizi di telefonia poteva archiviare i dati soltanto per finalità di natura commerciale, non incombendo in capo ad esso alcun obbligo di conservazione per esigenze di accertamento dei reati. Veniva a crearsi dunque una situazione paradossale secondo cui la pubblica autorità poteva acquisire i dati soltanto fino a quando questi risultassero utili per attività di fatturazione. Una volta venuto meno tale interesse di natura privatistica, i dati di traffico sarebbero stati automaticamente cancellati, a nulla rilevando l'eventuale necessità di apprensione da parte dell'autorità giudiziaria.

La normativa risultava ancora più inadeguata se si considerava che non tutti i dati potenzialmente utilizzabili in sede penale fossero fatturabili, con la conseguenza di una loro immediata cancellazione. In questi casi si verificava addirittura una preclusione assoluta della conoscibilità di tali informazioni e una soccombenza *in toto* dell'interesse costituzionalmente riconosciuto dell'accertamento dei reati. In sintesi, si realizzava una irragionevole subordinazione delle esigenze di pubblica sicurezza a quelle amministrativo-contabili dei gestori di servizi. Oltre a risultare del tutto ingiustificata, tale impostazione produceva un'ampia discrasia con quanto era stato poco prima affermato in sede pretoria. La possibilità di acquisire i dati di traffico secondo il procedimento illustrato nella giurisprudenza costituzionale veniva di fatto fortemente circoscritta alle condizioni stabilite dall'articolo 4 del d.lgs. 13 maggio 1998, n. 171.

3.1 I tabulati di traffico nel Codice *Privacy*: un primo approccio.

Le criticità prospettate poc'anzi sono state risolte con l'emanazione d.lgs. 30 giugno 2003, n. 196 (d'ora in poi Codice *Privacy*), che, per la prima volta, ha realizzato una disciplina organica e completa in materia di conservazione e di acquisizione dei dati di traffico[53]. L'intervento legislativo è stato sollecitato dalla legge comunitaria 306/2003[54] il cui art. 12 delegava il Governo a dare attuazione alla direttiva

[53] Così RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico*, *cit*., 170.
[54] Si fa riferimento alla legge 31 ottobre 2003, n. 306, recante «Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee. Legge comunitaria 2003» pubblicata in Gazzetta Ufficiale il 15 novembre 2003.

2002/58/CE[55] sulla tutela della vita privata nel settore delle comunicazioni elettroniche.

Attraverso la direttiva *de qua*, c.d. *e-Privacy*, il legislatore comunitario ha predisposto la tutela della riservatezza nell'ambito dei servizi telefonici e telematici stabilendo per i fornitori il divieto di ascoltare, registrare o effettuare altre forme di intercettazione delle conversazioni senza il consenso degli utenti[56]. In deroga a tale principio, l'articolo 15 della direttiva 2002/58/CE prevede che gli Stati possano disporre misure che aggirino tale divieto per ragioni di «salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati». In particolare, è consentita la l'archiviazione dei dati per un periodo di tempo limitato[57].

Come si è anticipato, il legislatore ha dato attuazione a tali previsioni comunitarie con l'emanazione del Codice *Privacy.* Tale impianto normativo, oggetto di molteplici interventi da parte legislatore, ha realizzato nel corso degli anni un costante contemperamento tra la tutela dei diritti fondamentali delle persone fisiche e lo sviluppo del mercato digitale e del progresso tecnologico[58]. Al suo interno, il Titolo X, Capo I[59], inerente alle "comunicazioni elettroniche" dedica una serie di articoli ai servizi telematici e al trattamento dei "dati di traffico".

Per le finalità del presente lavoro, è necessario innanzitutto fare riferimento all'articolo 123[60], il cui primo comma prevede l'obbligo del fornitore del servizio di

---

[55] La direttiva sopracitata, c.d. *e-Privacy*, detta norme inerenti al «trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)». È stata modificata con la direttiva 2009/136/CE e si inserisce nell'ambito di un ampio intervento del legislatore comunitario teso a garantire un livello omogeneo di tutela dei diritti fondamentali nel settore delle comunicazioni elettroniche. Per conseguire tale finalità, sono state emanate la direttiva quadro 21/2002/CE per le reti ed i servizi di comunicazione elettronica e altre quattro direttive attinenti a discipline complementari rispetto allo strumento legislativo principale. Tra di esse si annoverano, la direttiva 2002/20/CE «relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica»; la direttiva 2002/19/CE «relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate e all'interconnessione delle medesime»; la direttiva 2002/22/CE «relativa al servizio universale e ai diritti degli utenti in materia di reti e servizi di comunicazione elettronica»; la c.d. direttiva *e-privacy*. A tutte, tranne quest'ultima, è stata data attuazione nell'ordinamento italiano con il d.lgs. 2003, n. 259, Codice per le comunicazioni elettroniche.

[56] V. art 5 Direttiva 2002/58/CE.

[57] Per ulteriori approfondimenti sul contenuto della direttiva 2002/58/CE, si veda BUSIA, *Si volta pagina sulla tenuta dei tabulati telefonici*, in *Guida dir.*, 2003, 46, 40; VIGLIAR, Privacy *e comunicazioni elettroniche: la direttiva 2002/58/CE*, in *Dir. inf.*, 2003, 402.

[58] Si veda PELINO, ALAGNA, BOLOGNINI, *Codice della disciplina privacy*, Milano, 2019, 567.

[59] Si fa riferimento alla sequenza di articoli da 121 a 132-quater del Codice *Privacy*.

[60] L'art. 123, comma 1, del Codice *Privacy* prevede che «I dati relativi al traffico riguardanti contraenti ed utenti trattati dal fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione

traffico elettronico di cancellare o rendere immediatamente anonimi i dati di traffico qualora non siano più utili alla trasmissione della comunicazione[61]. In deroga a tale principio generale, i dati possono essere archiviati per un periodo di tempo non superiore a sei mesi al fine consentire al gestore di svolgere attività di fatturazione[62].

Emerge una evidente affinità tra la disciplina prevista dal d.lgs. 171/1998 e l'articolo 123 del Codice *Privacy*, che ne rappresenta "l'ideale continuazione ed evoluzione"[63]. Dal punto di vista sostanziale, l'unico elemento di novità della norma sopracitata consta nella previsione di periodo massimo di archiviazione dei dati per finalità di natura commerciale. Tale limite – rimasto tuttora invariato – non poteva superare le sei mensilità. Prima dell'emanazione del Codice *Privacy*, invece, i gestori potevano trattenere i dati di traffico senza alcuna restrizione temporale.

Oltre che per esigenze amministrative e contabili dell'ente gestore, si introduceva la possibilità di conservazione dei dati per finalità di repressione dei reati ai sensi dell'articolo 132. Nella sua versione originaria[64], tale articolo prendeva in considerazione soltanto i dati di traffico telefonico (escludendo quindi tutti quelli relativi a qualsiasi altra comunicazione elettronica) e stabiliva che fossero conservati dal gestore per trenta mesi. Si incaricava, inoltre, il Ministro della giustizia di concerto con i Ministri dell'interno e delle comunicazioni e su avallo del Garante della *Privacy*[65], di determinare con decreto le modalità di acquisizione dei dati all'interno

---

elettronica accessibile al pubblico sono cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunicazione elettronica, fatte salve le disposizioni dei commi 2, 3 e 5».

[61] I dati di traffico non possono essere più utilizzati dal gestore ai fini della trasmissione della comunicazione una volta che questa sia terminata. La conversazione telefonica tradizionale si intende "terminata" quando uno dei due utenti chiude il collegamento; nella messaggistica istantanea tramite posta elettronica, la trasmissione è completata nel momento in cui si ha la ricezione della *mail* da parte del destinatario.

[62] L'art. 123, comma 2, del Codice *Privacy* dispone che «Il trattamento dei dati relativi al traffico strettamente necessari a fini di fatturazione per il contraente, ovvero di pagamenti in caso di interconnessione, è consentito al fornitore, a fini di documentazione in caso di contestazione della fattura o per la pretesa del pagamento, per un periodo non superiore a sei mesi, salva l'ulteriore specifica conservazione necessaria per effetto di una contestazione anche in sede giudiziale».

[63] L'espressione è di RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico*, *cit*., *nota* 68.

[64] Per agevolare la comprensione di quanto detto *supra*, si ritiene utile riportare per intero l'art. 132, come introdotto dal d.lgs. 196/2003:
«Fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico telefonico sono conservati dal fornitore per trenta mesi, per finalità di accertamento e repressione di reati, secondo le modalità individuate con decreto del Ministro della giustizia, di concerto con i Ministri dell'interno e delle comunicazioni, e su conforme parere del Garante».

[65] Il Garante per la protezione dei dati personali, o Garante della *Privacy*, è un'autorità amministrativa indipendente italiana istituita, con legge 31 dicembre 1996, n. 675, al fine di garantire la tutela dei diritti

del procedimento penale. Inizialmente, gli aspetti processualpenalistici relativi alle modalità di acquisizione venivano dunque tralasciati e rimessi all'iniziativa dell'esecutivo.

Ancora prima della sua entrata in vigore, il Codice è stato modificato con il decreto-legge 24 dicembre 2003, n. 354 che ha completamente riscritto l'art. 132[66].

Innanzitutto, la versione rinnovata della norma prevedeva un'estensione della tipologia di dati suscettibili di acquisizione a fini probatori. Ai sensi del primo comma, non si faceva infatti più riferimento ai «dati relativi al traffico telefonico» ma più in generale a tutti i «dati relativi al traffico», ampliando notevolmente il raggio applicativo della norma. In tal modo, potevano essere archiviati ed eventualmente acquisiti non solo il traffico relativo alle telefonate ma anche quelli relativi ad ogni altro tipo di comunicazione telematica.

Un'altra novità della riforma è stata l'introduzione del "doppio binario"[67] per il periodo di conservazione dei dati[68]. Fermo restando l'obbligo di archiviazione dei dati di traffico per trenta mesi al fine dell'accertamento di qualsiasi fatto criminale, si prevedeva la possibilità di proroga di ulteriori trenta mesi esclusivamente per la

---

e delle libertà fondamentali nel trattamento dei dati personali. È composta da quattro membri eletti dal Parlamento, tra i quali viene nominato il Presidente.

[66] L'articolo 132 del decreto legislativo 30 giugno 2003, n. 196, era stato sostituito dal d.l. 354/2003 con il seguente, di cui si riportano i primi quattro commi:
«1. Fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico sono conservati dal fornitore per trenta mesi, per finalità di accertamento e repressione dei reati.

2. Decorso il termine di cui al comma 1, i dati sono conservati dal fornitore per ulteriori trenta mesi e possono essere richiesti esclusivamente per finalità di accertamento e repressione dei delitti di cui all'articolo 407, comma 2, lettera *a)* del codice di procedura penale, nonché dei delitti in danno di sistemi informatici o telematici.

3. Entro il termine di cui al comma 1, i dati sono acquisiti presso il fornitore con decreto motivato dell'autorità giudiziaria, d'ufficio o su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private. Il difensore dell'imputato o della persona sottoposta alle indagini può richiedere, direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'articolo 391-*quater* del codice di procedura penale.

4. Dopo la scadenza del termine indicato al comma 1, il pubblico ministero richiede al giudice, che decide con decreto motivato, l'autorizzazione ad acquisire i dati. Tale disposizione si applica anche al difensore dell'imputato o della persona sottoposta alle indagini che intenda acquisire direttamente i dati dal fornitore. Il giudice procede all'acquisizione, con decreto motivato, anche d'ufficio».

[67] L'espressione è di DE LEO, *La conservazione dei dati di traffico telefonico e telematico nella prospettiva europea*, in *Dir. pen. proc.*, 2002, 1016. L'Autore, tuttavia, dubita della coerenza di una simile logica perché, a differenza di quanto previsto per il regime "speciale" delle intercettazioni per indagini di criminalità organizzata, «altra cosa è prevedere che i dati che debbono comunque essere conservati vengano utilizzati per certe indagini per un periodo dimezzato rispetto ad altre».

[68] Cfr. art. 132, comma 2. Vedi *nota* 50.

repressione dei delitti previsti dall'articolo 407 comma 2 lett *a)* c.p.p., nonchè per quelli in danno di sistemi informatici o telematici[69].

Infine, il legislatore ha provveduto a colmare la maggiore lacuna della precedente versione dell'articolo in esame: per la prima volta è stata introdotta nell'ordinamento italiano una norma di natura processuale avente ad oggetto l'acquisizione dei tabulati. Anche la procedura di acquisizione rispettava la logica del doppio binario, poiché in base alla durata del periodo di conservazione dei dati veniva a corrispondere una bipartizione dell'*iter* acquisitivo.

Qualora l'attività di archiviazione fosse predisposta entro i limiti previsti dal primo comma, era possibile apprendere i dati per mezzo della procedura semplificata. Ai sensi dell'art. 132 comma 3, l'autorità giudiziaria aveva la possibilità di acquisire i dati mediante decreto motivato emesso d'ufficio o su istanza del difensore dell'imputato. In alternativa, il difensore dell'imputato poteva richiedere direttamente al fornitore dei servizi i dati intestati al proprio assistito in conformità con quanto previsto nel codice di procedura penale ai sensi dell'articolo 391-*quater* in materia di indagini difensive.

Nel caso in cui l'attività di archiviazione avesse ad oggetto i dati più risalenti nel tempo l'impianto normativo originario ne subordinava l'accesso all'avallo del giudice. Il quarto comma, da leggere in combinato disposto con il secondo, dettava dunque una disciplina specifica per l'acquisizione predisposta oltre i primi trenta mesi. Tale modalità prevedeva che chiunque ne chiedesse l'acquisizione, sia il pubblico ministero sia il difensore *ex* art. 391-*quater* c.p.p, dovesse ottenere l'autorizzazione del giudice che decideva con decreto motivato. Inoltre, rimaneva in capo all'autorità giurisdizionale la possibilità di acquisire i dati *ex officio*, in qualsiasi fase del procedimento[70].

---

[69] Sul punto si veda AMATO, *Il reato grave facilita l'accesso al tabulato*, in *Guida dir*., 2004, fasc. 2, 31. L'Autore sottolinea che i delitti in materia informatica sono stati equiparati alla criminalità grave per soddisfare «un'esigenza squisitamente investigativa, essendo evidente, per tali reati, l'utilità imprescindibile dell'acquisizione dei dati di traffico per acquisire elementi di prova essenziali, perché difficilmente surrogabili con altre iniziative investigative.

[70] Sottolinea che il potere officioso del giudice non era privo di limiti ma doveva rispettare le generali garanzie del processo penale (ad es. artt. 422 e 507 c.p.p.). AMATO, *Il reato grave facilita l'accesso al tabulato*, *cit.*, 32. In senso analogo, FRIGO, *Nella conservazione dei dati internet la necessaria tutela giurisdizionale*, in *Guida dir.*, 2004, n. 18, 14. In giurisprudenza v. Cass., Sez. VI, 11 febbraio 2002, n. 9331, Fortunato, in Cass. Pen., 2004, 1641, con nota di ARDITA.

Tale impostazione, secondo cui la maggiore complessità dell'*iter* acquisitivo risultava proporzionato alla durata del periodo di conservazione, si basava sull'assunto che la compressione del diritto alla riservatezza[71] non fosse sempre uguale. Al contrario, si riteneva che il *vulnus*[72] alla segretezza delle comunicazioni fosse più o meno intenso in ragione del "tempo" di durata dei dati di traffico. In correlazione al maggiore o minore disvalore del fatto veniva dunque a corrispondere un regime processuale semplificato (comma 3) e uno aggravato dal necessario intervento dell'autorità giurisdizionale (comma 4).

L'approccio sopra descritto, seppur condiviso da una parte della dottrina[73], così come il modello del "doppio binario", è stato abbondonato in tempi più recenti.

3.3 Le modifiche apportate dalla legge di conversione 26 febbraio 2004, n. 45.

La disciplina appena esaminata è stata modificata in sede di conversione dalla legge 26 febbraio 2004, n. 45[74], a riprova della persistente difficoltà del legislatore ad inquadrare l'istituto.

In primo luogo, la novella è intervenuta sull'ambito di applicazione della materia, circoscrivendola nuovamente al traffico telefonico, con l'esclusione dei dati relativi alle altre comunicazioni elettroniche. In secondo luogo, ha apportato una nuova modifica al periodo di archiviazione dei dati stabilendo un limite massimo di quarantotto mesi.

Durante il primo anno, l'acquisizione degli stessi veniva consentita per l'accertamento di qualsiasi di tipologia di reato; nei dodici mesi successivi era possibile procedere soltanto per la repressione di delitti di rilevante gravità[75] secondo il previgente modello del "doppio binario". L'intervallo di tempo durante il quale si

---

[71] CONTI, *L'attuazione della direttiva Frattini*, *cit.*, 11.

[72] L'espressione è di ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, *cit.*, 95.

[73] Riguardo alla logica del doppio binario e alla scelta di graduare la tutela del diritto alla riservatezza in base al tempo in cui si siano svolte le telefonate si è spesso in senso critico CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni, cit.,* 594.

[74] La legge sopra citata prevede «Disposizioni urgenti per il funzionamento dei tribunali delle acque, nonché interventi per l'amministrazione della giustizia» è stata pubblicata in Gazzetta Ufficiale il 27 febbraio 2004.

[75] Anche in questo si faceva riferimento ai delitti di cui all'articolo 407 comma 2, lett. *a)* c.p.p., nonché ai delitti in danno di sistemi informatici o telematici.

era protratta l'attività di custodia dei dati di traffico influiva sulla determinazione della procedura di acquisizione dell'autorità istante.

Nel primo caso, era necessaria l'emanazione di un decreto motivato da parte del P.M., che procedeva *ex officio* o su istanza del difensore dell'imputato secondo la modalità di cui all'articolo 391-*quater*. I dati conservati per più di dodici mesi invece potevano essere appresi soltanto in presenza di un'autorizzazione del giudice, il quale doveva accertare la sussistenza di «sufficienti indizi». In tal caso, l'*iter* di acquisizione era doppiamente aggravato dalla intermediazione dell'autorità giurisdizionale e da un consistente presupposto probatorio[76].

Inoltre, a differenza della disciplina previgente, non si prevedeva alcun potere di acquisizione *ex officio* in capo al giudice né una disciplina d'urgenza analoga a quella prevista per le intercettazioni. Ciò a riprova della definitiva autonomia che l'istituto suddetto aveva acquisito grazie alla creazione di *corpus* normativo a sé stante[77].

3.3 Le novità introdotte dal "decreto Pisanu".

Un ulteriore intervento sulla disciplina della *data retention* è stato realizzato con il decreto-legge 27 luglio 2005, n. 144, c.d. "decreto Pisanu"[78]. Il provvedimento *de quo* è stato emanato a seguito dei gravi attacchi terroristici di Madrid e Londra[79] per far fronte ai quali si predisponevano «Misure urgenti per il contrasto del terrorismo internazionale». Tra di esse, all'articolo 6 dell'atto sopracitato, figuravano «Nuove norme sui dati di traffico telefonico e telematico» che andavano a realizzare un nuovo

---

[76] Sul punto si veda GIORDANO, *Tabulati telefonici: senza regole sull'*iter *"convivenza" più difficile con la novella*, in *Guida dir.*, 2004, n.13, 12; PARODI, *Le modifiche del "d.l. giustizia" in tema di conservazione dei dati*, in *Dir. pen. Proc.*, 2004, 544.

[77] In tale senso RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico*, *cit.*, 170.

[78] Si fa riferimento al d.l. 144/2005, convertito con modificazioni dalla legge 31 luglio 2005, n. 155, contente una serie di norme relative all'utilizzo della Rete, predisposte per contrastare la criminalità e il proselitismo perpetrato per mezzo di strumenti informatici. In particolare, venivano vietate le connessioni anonime e si imponeva ai gestori di *Internet point* di redigere un archivio cartaceo con i nominativi dei propri utenti (art. 7 del d. l. 144/2005). Tale norma di natura transitoria, periodicamente rinnovata con il decreto milleproroghe, è stata abolita soltanto nel 2011. Altre norme del suddetto decreto sono tuttora vigenti. Per un approfondimento sul contenuto del decreto si veda KOSTORIS, *La lotta al terrorismo e alla criminalità organizzata tra speciali misure processuali e tutela dei diritti fondamentali nella risoluzione del XVIII Congresso internazionale del diritto penale*, in *Riv. dir. proc.*, 2010, 330.

[79] Si fa riferimento a due attentati terroristici di matrice islamica che hanno avuto grande risonanza europea e mondiale. Il primo ha avuto luogo l'11 Marzo 2004 a Madrid e ha causato la morte di 191 persone. Durante il secondo, il 7 Luglio 2005, quattro kamikaze si sono fatti esplodere in stazioni metro della capitale inglese causando la morte di 56 persone.

bilanciamento tra *data protection* e *data retention* in conseguenza delle contingenti esigenze di carattere transnazionale.

Nella norma *de quo* si riproponeva un modello bipartito nei tempi di conservazione non troppo distante da quello previgente, con l'aggiunta di una ulteriore differenziazione in base tipologia dei dati. Il primo termine di archiviazione era esteso a due anni per i dati di traffico telefonico, comprese le chiamate senza risposta; veniva invece limitato ad un semestre per i dati di traffico telematico, definitivamente inclusi nel raggio di applicazione della disciplina. Era predisposto un ulteriore tempo di conservazione della stessa durata – rispettivamente di ventiquattro (per il traffico telefonico) e sei mesi (per il traffico telematico) – per esclusive finalità di repressione di reati di particolare gravità. Rimaneva poi invariato il "doppio binario" relativo all'*iter* di apprensione dei tabulati all'interno del procedimento penale che veniva soltanto adeguato alle tempistiche sopra indicate.

Novità di maggior rilievo è stata, invece, l'introduzione di una procedura di emergenza analoga a quella esistente in materia di intercettazioni ai sensi dell'articolo 267, comma 2, c.p.p[80]. Il comma 4-*bis*[81] dell'art. 132 del Codice *Privacy* consentiva al pubblico ministero di predisporre l'acquisizione dei tabulati anche in assenza di preventiva autorizzazione del giudice in caso di «un grave pregiudizio alle indagini». L'autorità giurisdizionale doveva procedere alla convalida del decreto del P.M. entro quarantotto ore dalla sua emanazione, pena l'inutilizzabilità sopravvenuta dei dati appresi.

[80] L'art. 267, comma 2, c.p.p. dispone che «Nei casi di urgenza, quando vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini, il pubblico ministero dispone l'intercettazione con decreto motivato, che va comunicato immediatamente e comunque non oltre le ventiquattro ore al giudice indicato nel comma 1. Il giudice, entro quarantotto ore dal provvedimento, decide sulla convalida con decreto motivato. Se il decreto del pubblico ministero non viene convalidato nel termine stabilito, l'intercettazione non può essere proseguita e i risultati di essa non possono essere utilizzati».

[81] Ai sensi dell'art. 132, comma 4-*bis*, si prevedeva che «Nei casi di urgenza, quando vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini, il pubblico ministero dispone la acquisizione dei dati relativi al traffico telefonico con decreto motivato che è comunicato immediatamente, e comunque non oltre ventiquattro ore, al giudice competente per il rilascio dell'autorizzazione in via ordinaria. Il giudice, entro quarantotto ore dal provvedimento, decide sulla convalida con decreto motivato. Se il decreto del pubblico ministero non è convalidato nel termine stabilito, i dati acquisiti non possono essere utilizzati».

Sebbene coerente con la necessità di semplificare l'*iter* di acquisizione dei tabulati, tale disciplina ha avuto vita molto breve in quanto i commi 4 e 4-*bis* sono stati abrogati meno di tre anni dopo dal decreto legislativo 109/2008[82].

3.4 L'introduzione della procedura "di congelamento" da parte della legge di ratifica della Convenzione di Budapest.

La cronistoria degli interventi legislativi succedutisi in tema di dati esteriori sarebbe incompleta se si tralasciasse di far riferimento alla legge 18 marzo 2008, n. 48 di esecuzione della Convenzione del Consiglio D'Europa sulla criminalità informatica[83]. Con la novella legislativa *de quo*[84]*,* si è provveduto alla modifica di numerosi articoli del codice di procedura penale al fine di adeguarli alle nuove istanze processuali[85] in materia di *Cybercrime.*

Inoltre, si è realizzata un'interpolazione dell'articolo 132 del Codice *Privacy* mediante l'aggiunta dei commi 4-*ter*, 4-*quater* e 4-*quinquies*[86]. Tali disposizioni,

---

[82]Entrambi i commi sono stati abrogati dall'art. 2, comma 1, lett. c), d. lgs. 30 maggio 2008, n. 109 a cui si rinvia.

[83] La Convenzione del Consiglio d'Europa sulla criminalità informatica, cd. *Convention on Cybercrime*, (spesso in acronimo CoC), è stata redatta il 23 novembre 2001. Il risultato è il frutto di quattro anni di lavori durante i quali hanno partecipato anche Stati extraeuropei (Canada, Stati Uniti e Giappone) di rilevanza strategica, la cui collaborazione era essenziale a realizzare una politica comune e dicooperazione internazionale in campo di criminalità informatica (v. preambolo). È il primo trattato internazionale sulle fattispecie criminose perpetrate mediante Internet e le altre reti informatiche. Prevede al suo interno norme di diritto penale sostanziale e processuale che si applicano non solo ai reati da essa stessa definiti, ma anche a qualsiasi altro delitto perpetrato mediante accesso ad un sistema informatico, nonché una disciplina organica sulle "prove in forma elettronica" (art 14, comma 2 ed art 23 CoC).

[84] Per approfondire, si veda PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Legge 18 marzo 2008, n. 48, in Diritto penale e processo, 2008,* n. 6, 696*;* LUPARIA, *La ratifica della Convenzione* Cybercrime *del consiglio d'Europa*, in *Dir. pen e proc*., 2008, 721.

[85] A titolo meramente esemplificativo si veda l'inserimento dell'articolo 254bis c.p.p. in materia di sequestro di dati informatici, di cui si tratterà *infra.*

[86]Di seguito, si riportano i commi sopracitati dell'art. 132 attualmente vigenti:
«Il Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonché gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al *decreto legislativo 28 luglio 1989, n. 271*, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al *decreto legislativo n. 271 del 1989*, ovvero per finalità di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere

rimaste invariate nel testo vigente, prevedono una speciale disciplina in tema di conservazione dei tabulati.

La procedura *de qua*, denominata di "congelamento" (c.d. *quick freeze procedure*)[87], viene messa in moto tramite un ordine emanato da soggetti dotati di funzioni esecutive ai sensi dell'articolo 226, comma 1 delle Disposizioni di attuazione del codice di procedura penale. Tra di essi figurano il Ministro dell'interno, i responsabili degli uffici specializzati della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza. I soggetti di cui sopra possono ordinare ai fornitori di servizi di comunicazione elettronica la conservazione dei dati di traffico telematico, per un periodo di tempo non superiore a novanta giorni, prorogabile fino a sei mesi laddove sussistano «motivate esigenze».

L'emanazione dell'ordine di esecuzione, redatto necessariamente per iscritto, è finalizzata al soddisfacimento di interessi investigativi interni o manifestati da autorità straniere. L'operatore di servizi destinatario del provvedimento è tenuto ad adempiervi immediatamente e a non divulgare a terzi la ricezione dello stesso; in caso contrario, sarà penalmente perseguibile ai sensi dell'articolo 326 del codice penale per rivelazione ed utilizzazione di segreti d'ufficio, salvo la sussistenza più grave reato[88].

Entro quarantotto ore dalla notifica al gestore dei servizi, il pubblico ministero del luogo dell'esecuzione, se rileva la sussistenza dei presupposti, procede alla convalida

---

particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi (comma 4-*ter*).
Il fornitore o l'operatore di servizi informatici o telematici cui è rivolto l'ordine previsto dal comma 4-ter deve ottemperarvi senza ritardo, fornendo immediatamente all'autorità richiedente l'assicurazione dell'adempimento. Il fornitore o l'operatore di servizi informatici o telematici è tenuto a mantenere il segreto relativamente all'ordine ricevuto e alle attività conseguentemente svolte per il periodo indicato dall'autorità. In caso di violazione dell'obbligo si applicano, salvo che il fatto costituisca più grave reato, le disposizioni dell'articolo 326 del codice penale (comma 4-*quater*).
I provvedimenti adottati ai sensi del comma 4-ter sono comunicati per iscritto, senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione il quale, se ne ricorrono i presupposti, li convalida. In caso di mancata convalida, i provvedimenti assunti perdono efficacia (4-*quinquies*)».

[87] V. RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico*, cit., 183.

[88] Cfr. art. 132, comma 4-*quater*. In dottrina è stato rilevato che si tratti di una sanzione eccessivamente severa, che per di più penalizzi soltanto il soggetto attivo che integra la condotta diffusiva, tralasciando del tutto il soggetto passivo. Tale scelta di politica criminale si spiega se si tiene conto della logica preventiva alla base di tale tipologia di reati. Sul punto si veda, ATERNO, *Conservazione dei dati informatici e prospettive europee. Relazione svolta al Convegno dell'OLAF (Milano, 23-25 gennaio 2008),* Milano, 2009, 163.

dell'istanza. In assenza di tale provvedimento di omologa l'istanza è improduttiva di effetti[89].

Dall'analisi della disciplina appena enucleata emergono una serie di criticità di carattere sistematico che ne precludono una comprensione chiara e immediata. La lacuna più evidente si ha nella determinazione dei presupposti sostanziali per l'emanazione dell'ordine di esecuzione. Ai sensi del comma 4-*ter,* la procedura di cui trattasi può essere attivata per «specifici reati» di cui però non si provvede a fornire una definizione. Per cogliere la portata di tale espressione è necessario fare riferimento all'articolo 226[90] disp. att. c.p.p. in materia di investigazioni preventive, il cui combinato disposto con l'articolo 132 Codice *privacy* realizza una tassatività *per relationem*[91].

Se mediante tale ricorso *extra codicem* si riesce a sopperire alla lacuna appena emersa, incolmabile è il vuoto relativo agli altri elementi oggettivi. In particolare, appare del tutto indeterminato il riferimento alla sussistenza di «finalità investigative» per l'emanazione dell'ordine di esecuzione e alle «motivate esigenze» che devono subentrare per disporne una proroga.

Inoltre, il legislatore non specifica i presupposti istruttori che legittimino l'emanazione dell'ordine di congelamento. Sul punto, la dottrina si è interrogata se sia sufficiente che l'autorità giudiziaria sia in possesso di generici indizi di reato o se invece sia necessaria la sussistenza del *fumus commissi delicti.* Secondo tale impostazione maggiormente garantista, l'adozione della procedura di urgenza verrebbe giustificata soltanto in presenza di elementi probatori di una certa consistenza.

Di seguito, è opportuno osservare che un altro aspetto problematico dell'impianto normativo in esame consiste nella totale assenza di coordinamento con i precedenti commi della medesima norma del Codice *Privacy*. I commi 4-*ter*, 4-*quater* e 4-*quinquies* sembrano infatti prevedere una procedura di conservazione ulteriore rispetto a quella ordinaria prevista dall'articolo 132. Tale impostazione è confermata dal fatto

[89] Cfr. art. 132, comma 4-*quinquies*.
[90] Nell'art. 226, comma 1 disp. att. c.p.p., rubricato «intercettazioni e controlli preventivi sulle ccomunicazioni» si fa riferimento ai delitti in materi di terrorismo internazionale e criminalizzata ai sensi degli artt. 407 comma 2 lett. a) n. 4 e 51 comma 3-*bis* c.p.p.
[91] L'espressione è di CONTI, *L'attuazione della direttiva*, cit., 23.

che nella disciplina "di congelamento" si fa riferimento soltanto all'attività di archiviazione, mentre non si dice nulla in merito a quella di acquisizione.

In assenza di apposita specificazione, si dovrebbe applicare *de residuo* la disciplina processuale prevista dal terzo comma. Una volta emanato l'ordine di congelamento dei dati, l'autorità competente potrebbe procedere all'acquisizione dei dati nel rispetto dei tempi e delle modalità previste dalla disciplina ordinaria. Il mancato coordinamento tra le due norme porta con sé il rischio che su questa interpretazione garantista possa prevalerne una più lassista. La procedura in esame potrebbe infatti essere utilizzata come un espediente per ottenere una sorta di prolungamento straordinario dei limiti temporali previsti dai primi commi.

Un'ultima criticità riguarda l'individuazione del novero dei soggetti destinatari dell'ordine di conservazione[92]. Mentre l'articolo 132 del Codice *Privacy* si rivolge soltanto ai gestori di servizi di comunicazione elettronica, rientrano nell'ambito di applicazione della Convenzione di Budapest e della legge di ratifica anche "gestori dei siti Internet che diffondono contenuti sulla rete" c.d. *content provider*. Nonostante tale discrasia non sia stata esplicitamente risolta dal legislatore, ostacola l'inclusione di questi ultimi tra i potenziali destinatari dell'ordine di archiviazione il fatto che l'operazione di *data retention* non ha mai ad oggetto il contenuto delle comunicazioni. Un'apertura su tale aspetto da parte del legislatore rappresenterebbe infatti una deroga vistosa rispetto alla *ratio* dell'istituto[93].

Sulla base di quanto esposto, risulta evidente che la norma – rimasta invariata nella disciplina attualmente vigente – sia connotata da una vaghezza semantica eccessiva. L'imprecisione riscontrata in fase redazionale non soltanto ostacola un'agevole attuazione della procedura descritta ma porta con sé il rischio di attribuire agli organi dell'esecutivo un potere di fatto molto esteso e potenzialmente suscettibile di utilizzo arbitrario.

---

[92] RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico*, *cit.*, 183.

[93] Così ATERNO, *Commento all'art. 10*, in AA. VV., *L'attuazione della Convenzione di europea sul cybercrime. Commento alla legge 18 marzo 2008 n.48*, Milano, 2008, 70; IBIDEM, *Conservazione dei dati informatici e prospettive europee, cit., 162.*

3.5 L'attuazione della direttiva 2006/24/CE.

Ancora una volta, la spinta propulsiva verso nuove istanze di riforma in tema di *data retention* ha avuto origine comunitaria. Mediante l'emanazione della direttiva 2006/24/CE, c.d. "direttiva Frattini"[94], il legislatore europeo si è occupato per la prima volta in esclusiva della disciplina di conservazione dei dati «a fini di indagine, accertamento e perseguimento di reati gravi»[95] con l'obiettivo di armonizzare le disposizioni nazionali.

Nel dare attuazione all'articolo 15 della direttiva *e-Privacy*[96], gli Stati membri avevano infatti emanato discipline tra loro fortemente disomogenee sia riguardo alle tipologie di dati da conservare, sia rispetto alla durata di tale attività di archiviazione. La carenza di uniformità tra le normative nazionali entrava in contraddizione con gli obiettivi eurounitari mettendo a rischio il mercato interno delle comunicazioni elettroniche[97].

Per risolvere tali discrasie sul piano giuridico e tecnico, il Parlamento europeo e il Consiglio hanno emanato un atto legislativo[98] che lasciasse pochi margini di discrezionalità nel recepimento da parte dei singoli Stati. All'interno dell'ordinamento italiano si è dato attuazione alla direttiva sopracitata con il d.lgs. 109/2008[99], che ne

---

[94] Si fa riferimento alla direttiva del Parlamento europeo e del Consiglio del 15 marzo 2006 «riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione». Tra gli studiosi lo strumento è conosciuto anche come "direttiva Frattini".

[95] Cfr. art 1 della direttiva 2006/24/CE.

[96] V. *supra*, Cap. I, § 3.5.

[97] In tal senso, CONTI, *L'attuazione della direttiva Frattini*, *cit.*, 2008, 14.

[98] Per quanto concerne il contenuto della direttiva, in questa sede basti ricordare che l'articolo 2 della stessa forniva una serie di definizioni in materia di comunicazioni elettroniche andando ad integrare quelle già presenti nelle direttive 95/46/CE, 2002/21/CE e 2002/58/CE, esplicitamente richiamate. Il perno dell'intera disciplina era però rappresentato dall'articolo 6 che determinava l'intervallo di tempo (tra i sei mesi e i due anni) entro il quale gli Stati potevano stabilire il periodo di archiviazione dei dati di traffico. Tale norma andava letta in combinato disposto con la clausola di riserva contenuta nell'articolo 12 secondo cui ciascuno Stato membro poteva prorogare le tempistiche anzidette per un periodo limitato e in presenza di «circostanze particolari». La deroga era stata pensata per garantire gli strumenti necessari a livello nazionale per fare fronte ad eventuali attentati terroristici. D'altronde, la stessa direttiva 2006/24/CE era nata in risposta agli attacchi terroristici di Londra (Cfr. Considerando 10). Per un maggiore approfondimento sul punto v. Cap. II.

[99] Nonostante la direttiva dovesse essere attuata entro il 15 settembre 2007, agli Stati membri veniva concessa la possibilità di differirne l'applicazione fino al 15 marzo 2009 (ai sensi dell'articolo 15 paragrafo 3). In controtendenza rispetto alla maggioranza degli Stati membri (tra cui Austria, Belgio, Cipro, Estonia, Finlandia, Germania, Grecia, Lettonia, Lituania, Lussemburgo, Olanda, Polonia, Regno Unito, Repubblica Ceca, Slovenia, Svizzera, Svezia) l'Italia ha deciso di non avvalersi di tale facoltà, introducendo la direttiva con legge comunitaria 13/2007, cd. "legge comunitaria 2006".

ha riproposto pedissequamente il contenuto sia sul piano definitorio sia su quello prescrittivo.

Tra gli interventi di maggior rilievo, basti qui ricordare che la novella è intervenuta sia sulla nozione di «dati di traffico» sia su quella di «traffico telefonico», estendendone la portata fino ad includere le chiamate tramite la rete *Internet*. Sul piano processuale, ha realizzato invece una *reductio ad unum* delle modalità di apprensione dei dati eliminando il previgente sistema del "doppio binario"[100]. Ciò ha determinato il passaggio da un meccanismo di acquisizione estremamente articolato ad un regime semplificato caratterizzato da un accentramento di competenze in capo alla figura del pubblico ministero[101]. Tale soluzione normativa è rimasta invariata nella disciplina tuttora vigente e sarà a suo tempo oggetto di una disamina approfondita[102].

In questa sede, è necessario invece proseguire nell'analisi dell'evoluzione legislativa, facendo riferimento agli accadimenti intervenuti a seguito dell'emanazione della 2006/24/CE. Nonostante la solerzia del legislatore italiano nell'attuazione della stessa, il suo contenuto altamente invasivo la sfera dei diritti fondamentali aveva creato un ampio dibattito a livello europeo[103]. A riprova di ciò, decorso meno di un anno dalla sua entrata in vigore, è stata oggetto di una richiesta di annullamento davanti alla Corte europea di giustizia da parte dell'Irlanda nel caso c.d. *Digital Rights Ireland Ltd e Seitlinger*. Il giudizio si è concluso soltanto nel 2014 con una pronuncia di accoglimento in cui si dichiarava invalida la c.d. direttiva Frattini, in quanto incompatibile con gli artt. 7, 8, 52, co. 1, della Carta di Nizza[104]. La controversia ha avuto ampia risonanza non solo per quanto stabilito in materia di *data retention* ma soprattutto per i principi affermati in tema di protezione dei dati personali.

[100] L'espressione è di RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico*, *cit.*, 182.
[101] Si veda ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, *cit.*, 94.
[102] Cfr. Cap. I § 4.3.
[103] Sul punto MARCOCCIO, Data retention*, la "Pisanu" dovrà fare i conti con l'Europa*, in *www.interlex.it.*
[104] Per un esame completo della sentenza Cfr. Cap. II.

3.6 Le novità introdotte dal "decreto antiterrorismo".

Il più recente intervento normativo in tema di conservazione dei dati telefonici è occorso in prossimità dei tragici attentati di Parigi[105]. Tale evento storico-politico ha avuto una risonanza così rilevante da condizionare la formazione legislativa successiva nel quadro europeo e nazionale. A conferma di ciò, il governo italiano ha emanato il decreto-legge 7/2015[106] recante «Misure urgenti per il contrasto del terrorismo, anche di matrice internazionale, nonché proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle Organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione».

In tale contesto, si inserisce l'ulteriore sedimentazione normativa avente ad oggetto l'articolo 132 del Codice *Privacy,* mediante la quale viene introdotto un regime derogatorio rispetto alla ordinaria disciplina di *data storage*.

L'articolo 4-*bis* del d.l. 7/2015[107] disponeva infatti che i dati di traffico telefonico, telematico e le chiamate senza risposta effettuate a partire dall'entrata in vigore della

---

[105] Si fa riferimento ad una serie di attacchi terroristici di matrice islamica che sono stati perpetrati il 13 novembre 2015 nella capitale francese, in seguito rivendicati dall'autoproclamato Stato Islamico, comunemente noto come ISIS. Tra le aggressioni, tre esplosioni nei pressi dello stadio e sei sparatorie in diversi luoghi pubblici, la più sanguinosa delle quali è avvenuta presso il teatro *Bataclan* dove sono rimaste uccise 90 persone. Si è trattato di un'aggressione così cruenta da far dichiarare all'allora in carica Presidente della Repubblica francese *François Hollande*, lo stato di emergenza e la provvisoria chiusura delle frontiere.

[106] Con il decreto-legge 18 febbraio 2015, n.7, convertito con modificazioni dalla legge 17 aprile 2015, n. 43, il legislatore italiano si è posto l'obiettivo di potenziare gli strumenti di contrasto al terrorismo internazionale privilegiando una logica di prevenzione. Per conseguire tale finalità, ha stabilito l'ampliamento le prerogative del personale operante nelle agenzie governative dell'*intelligence*, con particolare attenzione al crescente fenomeno dei *foreign fighters.* Tra le nuove norme di carattere processuale, è opportuno fare cenno all'accentramento delle indagini in capo al Procuratore nazionale antimafia. Per un maggiore approfondimento sul c.d. "pacchetto antiterrorismo" si veda KOSTORIS, *Il nuovo pacchetto antiterrorismo, tra prevenzione, contrasto in rete e centralizzazione delle indagini*, KOSTORIS - VIGANO', Il nuovo pacchetto antiterrorismo, Torino, 2015, XV.

[107] L'art. 4-bis del d.l. 7/2015, rubricato «Disposizioni in materia di conservazione dei dati di traffico telefonico e telematico», prevedeva che:

«1. Al fine di poter agevolare le indagini esclusivamente per i reati di cui agli articoli 51, comma 3-quater, e 407, comma 2, lettera *a)*, del codice di procedura penale, in deroga a quanto stabilito dall'articolo 132, comma 1, del codice di cui al decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni, e fermo restando quanto stabilito dall'articolo 123, comma 2, del medesimo codice, i dati relativi al traffico telefonico effettuato a decorrere dalla data di entrata in vigore della legge di conversione del presente decreto sono conservati dal fornitore fino al 31 dicembre 2016 per finalità di accertamento e repressione dei reati. Per le medesime finalità i dati relativi al traffico telematico effettuato a decorrere dalla data di entrata in vigore della legge di conversione del presente decreto, esclusi comunque i contenuti della comunicazione, sono conservati dal fornitore fino al 31 dicembre 2016.

2. I dati relativi alle chiamate senza risposta, effettuate a decorrere dalla data di entrata in vigore della legge di conversione del presente decreto, trattati temporaneamente da parte dei fornitori di servizi di

legge di conversione dovevano essere archiviati fino al 31 Dicembre 2016[108]. Tale dilatazione generalizzata degli ordinari tempi di conservazione, veniva realizzata al fine di agevolare le attività di indagine degli organi inquirenti. Eppure, l'obiettivo *de quo* è stato di fatto vanificato da una serie di incongruenze riscontrate in fase redazionale che hanno poi generato difficoltà in sede di applicazione.

Innanzitutto, è necessario sottolineare l'irragionevolezza di una duplice indicazione del profilo teleologico[109] all'interno della medesima norma. Mentre nell'*incipit* dell'articolo 4-*bis* si parla, infatti, di «agevolare le indagini esclusivamente per i reati di cui agli articoli 51, comma 3-quater, e 407, comma 2, lettera *a)*[110], del codice di procedura penale», al secondo comma figurava l'espressione più generica «accertamento e repressione dei reati».

Di fronte a tale evidenza, la dottrina si è interrogata a lungo su quale fosse l'espressione a cui fare riferimento per la determinazione dell'ambito di applicazione della disciplina. Non era infatti chiaro se i tempi di conservazione di natura derogatoria dovessero applicarsi in qualsiasi indagine o soltanto nelle investigazioni aventi ad oggetto i reati in materia di terrorismo internazionale e di criminalità organizzata. In dottrina si tende a preferire questa seconda soluzione perché l'unica compatibile con i principi di necessità e proporzionalità enunciati dalla giurisprudenza della Corte di Lussemburgo[111].

Secondo tale ottica, l'introduzione di norme derogatorie e potenzialmente più invasive nella sfera di riservatezza dell'individuo viene giustificata soltanto se circoscritta alla repressione di delitti che mettono in serio pericolo la sicurezza nazionale. Ne consegue che una disciplina che postula una estensione dei tempi di *data storage* – e di conseguenza un sacrificio maggiore della tutela della segretezza delle

---

comunicazione elettronica accessibile al pubblico oppure di una rete pubblica di comunicazione, sono conservati fino al 31 dicembre 2016.
3. Le disposizioni di cui ai commi 1 e 2 cessano di applicarsi a decorrere dal 1° gennaio 2017»
Siffatta normativa è entrata in vigore il 21 aprile 2015.

[108] La medesima data ricorre nella c.d. *sunset clause* del *Data retention and Investigatory Powers Act 2014* (in acronimo DRIP O DRIPA) adottato dal Regno Unito per far fronte all'emergenza terroristica. Per consultare online il testo citato si veda *www.legislation.gov.uk.*

[109] RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico*, *cit.*, 189.

[110] L'articolo 407 lett. *a)* del codice di procedura penale fa un lungo elenco di gravi reati a cui si rimanda. In generale, rientrano in tale categoria i reati commessi al fine di agevolare associazioni criminalità organizzata nonché reati commessi per finalità di terrorismo o di eversione dell'ordinamento costituzionale.

[111] Cfr. Cap II.

comunicazioni – è considerata legittima soltanto se limitata a reati di particolare gravità.

Ciò posto, è necessario verificare se l'introduzione di tale disciplina "eccezionale" abbia effettivamente avvantaggiato le esigenze di investigazione e di accertamento dei reati. In merito a ciò, emergono infatti numerose criticità[112].

La dottrina ha rilevato che l'impianto normativo introdotto dall'art. 4-*bis* del d.l. 7/2015, almeno nella sua versione originaria, abbia in alcuni casi determinato una riduzione dei tempi di conservazione, ottenendo un effetto contrario rispetto a quanto predisposto. Per capire come si sia potuto incappare in tale equivoco è necessario far riferimento ai lavori preparatori dell'atto legislativo in esame[113].

La *ratio* originaria della norma prevedeva un superamento della divisione nelle diverse categorie di dati – punto poi correttamente attuato – e un'estensione generalizzata dei tempi di conservazione fino a ventiquattro mesi per le comunicazioni elettroniche effettuate tra il 21 aprile 2015 e il 31 Dicembre 2016. La data da ultimo menzionata era dunque riferita all'arco temporale entro cui dovevano essere effettuate le chiamate per rientrare nell'ambito di applicazione del presente decreto.

Con l'approvazione del testo definitivo della norma, però, il termine di ventiquattro mesi è sorprendentemente venuto meno e la fine del periodo di archiviazione è stata identificata con il 31 Dicembre 2016. Come conseguenza di questa irragionevole soppressione, l'effetto benefico di estensione dei tempi di conservazione si otteneva soltanto quando il lasso di tempo tra la data della comunicazione e il 31 Dicembre 2016, giorno ultimo di conservazione, risultava superiore alle soglie ordinarie previste dall'articolo 132 (di 24 mesi, 12 mesi o 30 giorni). Quando invece la comunicazione era stata effettuata molto a ridosso della data suindicata, i tempi di conservazione risultavano addirittura ridotti e le prerogative di indagine compromesse.

Nel tentativo di rimediare a tale svista, il legislatore[114] estendeva i tempi di conservazione straordinari «fino al 30 giugno 2017». Nonostante tale proroga,

---

[112] Cfr. CAPUTO, *La conservazione dei dati di traffico telefonico e telematico nella normativa antiterrorismo*, in *Archivio penale*, 2016, n.1, 28.

[113] Sul punto si veda Senato della Repubblica, *Fascicolo Iter DDL. S. 1854 – 1.4.2.4.1. 10a Commissione permanente (Industria, commercio, turismo)* – Seduta n. 133 (pom.), 8 aprile 2015, in cui si specificava, in relazione all'articolo 4-*bis*, l'equiparazione dei termini di conservazione (ventiquattro mesi) dei dati di traffico telefonico, telematico e delle chiamate senza risposta.

[114] Tale estensione è stata realizzata dall'art 4-*bis* del decreto 30 dicembre 2015, n. 210, c.d. Mille-proroghe, convertito con modifiche dalla legge 25 febbraio 2016, n. 21.

rimanevano però valide tutte le incongruenze sopra segnalate, dal momento che l'impianto originario della disposizione in esame era rimasto invariato.

Ne conseguiva che i dati delle comunicazioni elettroniche effettuate a ridosso della data suindicata continuavano ad essere conservati per un periodo inferiore a quello previsto dall'articolo 132, con una grave compromissione delle esigenze di indagine.

L'intervento correttivo del legislatore si era dunque rivelato soltanto un tentativo non riuscito di porre fine all'interferenza tra i termini della disciplina originaria. In assenza di un nuovo provvedimento di proroga, la disciplina in esame non risulta più vigente a partire dal 1° luglio 2017.

4. La disciplina attuale: esegesi dell'articolo 132 del Codice *Privacy*, da ultimo modificato dal d.lgs. 101/2018.

La ricognizione del quadro normativo sin qui esaminato attesta che la disciplina della c.d. *data retention,* espressamente regolamentata nel Codice *Privacy*, è stata segnata da una parabola evolutiva ciclicamente oscillante. Tale estrema instabilità è cagionata eminentemente da una profonda permeabilità dell'istituto al contesto socioculturale dominante, nazionale e comunitario. La gran parte degli interventi del legislatore italiano, aventi ad oggetto l'articolo 132 Codice *Privacy,* sono stati infatti la risultante di scelte politiche profondamente contingenti e influenzate dagli avvenimenti storici più rilevanti dello scorso decennio[115]. In particolar modo, si è visto come il terrorismo internazionale, che ha generato una pervasiva sensazione di allarme e di paura in tutta Europa, abbia giocato un ruolo fondamentale nel rafforzare le istanze di sicurezza.

La costante ricerca di un punto di equilibrio tra esigenze contrapposte ha impedito la sedimentazione di una normativa stabile e idonea a salvaguardare tutti i diritti fondamentali coinvolti. Con l'auspicio che, nei prossimi anni, l'atteggiamento altalenante del legislatore subisca una battuta d'arresto, realizzando un inquadramento definitivo della materia di cui trattasi, è opportuno rivolgere l'attenzione alla disciplina attuale.

---

[115] Cfr. ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, cit., XIV.

Ad oggi, l'ultima rilevante modifica[116] al Codice *privacy*[117], che ha ridisegnato l'intera materia, è stata apportata dal d.lgs. 10 agosto 2018, n. 101[118], in attuazione del "pacchetto europeo protezione dei dati"[119]. Con il decreto sopracitato, il Governo italiano ha dato esecuzione alla delega prevista all'articolo 13 della legge 163/2017[120],

[116]Per completezza espositiva si segnala che, dopo la novella del 2018, il legislatore è nuovamente intervenuto sul Codice *Privacy* con la legge di Bilancio 2020. L'articolo 1 comma 681 della l. 160/2019 modifica l'articolo 2-*sexies*, comma 2 del d.lgs. 196/2003 introducendo una nuova fattispecie di trattamenti di dati personali derivanti dall'attività di soggetti pubblici di prevenzione e contrasto all'evasione fiscale. In conseguenza di tale interpolazione, i diritti dell'interessato previsti dagli articoli dal 15 al 22 del GDPR (diritto di accesso dell'interessato, diritto di rettifica, diritto di opposizione *etc. etc.*) non possono essere esercitati in materia tributaria. Ai fini della presente ricerca, non risulta utile dilungarsi oltre sull'intervento *de quo* che ha lasciato inalterata la previgente disciplina della *data retention.*

[117]Attualmente «Codice *Privacy* in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (Ue) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE».

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

[119]A partire dal 2012, in ambito europeo era stato avviato un *iter* legislativo di larga scala con l'obiettivo di ripensare l'intera materia del trattamento dei dati personali alla luce di nuove esigenze emerse con il progresso tecnico-scientifico. Tale produzione normativa ha dato luogo all'emanazione del sopracitato "pacchetto europeo protezione dei dati", di cui fanno parte tre differenti atti:

1) «Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE» (c.d. Regolamento generale sulla protezione dei dati o *General Data Protection Regulation,* in acronimo GDPR). In base all'articolo 99, comma 2, il regolamento è direttamente applicabile in tutti gli Stati membri a partire dal 25 maggio 2018, in differita rispetto alla sua entrata in vigore, rispettivamente il 24 maggio 2016.

2) «Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio». Tale direttiva è entrata in vigore il 5 maggio 2016 con l'obbligo di recepimento per gli Stati membri entro il 6 maggio 2018. Incidendo su una materia particolarmente delicata, essa si pone l'obiettivo di realizzare un migliore contemperamento delle esigenze di accertamento penale con la tutela della *privacy*. Per un approfondimento della direttiva, cfr. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018, 87 ss.

3) «Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi». Per un approfondimento sui *Passenger name record* e su come l'accesso a tali dati possa costituire un importante strumento di tutela per contrastare la criminalità transnazionale si veda ROSSI, *Gli accordi PNR ("Passenger Name Record") nella lotta al terrorismo internazionale. Conseguenze del parere n. 1/15 della Corte di giustizia del 26 luglio 2017 per la legittimità della Direttiva n. 2016/681/Ue*, in *Dir. comun. e degli scambi int.*, 2018, fasc. 3, 395 e ss.

[120] Si fa riferimento alla legge di delegazione europea 25 ottobre 2017, n. 163. Ai sensi dell'articolo 13 tale atto forniva una «Delega al Governo per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE».

adeguando il quadro normativo nazionale a quello europeo in materia di *privacy*, e in particolar modo al GDPR.

Con tale ultimo atto, la Commissione europea si è posta l'obiettivo di semplificare e rendere omogenea tra gli Stati membri la disciplina relativa al «trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi»[121]. Tale attività deve essere realizzata nel totale rispetto dei diritti e delle libertà fondamentali delle persone fisiche – e non anche delle persone giuridiche[122] – con particolare riguardo al diritto alla protezione dei dati personali. Ai sensi dell'articolo 3[123], il GDPR si applica ad ogni titolare o responsabile del trattamento che abbia sede all'interno dell'Unione, indipendentemente dal fatto che il trattamento medesimo sia effettuato o meno in territorio comunitario. Restano però espressamente esclusi dal raggio di applicazione della norma quattro tipologie di trattamenti: le attività che non rientrano nel campo di applicazione del diritto europeo; quelle realizzate in relazione alla politica estera e di sicurezza comune[124]; i trattamenti operati da una persona fisica ad utilizzo esclusivamente personale o domestico[125]; da ultimo, i trattamenti effettuati da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali[126]. Dall'ultima proposizione si deduce che il GDPR non si applica in tema di *data*

[121] Cfr. Art. 2 Regolamento (UE) 2016/679.
[122] Sull'esclusione dal raggio di applicazione del sopracitato regolamento si esprime chiaramente il Considerando 14 riportato di seguito «È opportuno che la protezione prevista dal presente regolamento si applichi alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali. Il presente regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto».
[123]Si ritiene utile riportare per intero, l'art. 3, paragrafo 1, del GDPR secondo cui: «Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione». Per una puntuale esegesi di tale norma e un approfondimento sull'applicazione extraterritoriale del GDPR si veda BOLOGNINI, PELINO, BISTOLFI, *Il regolamento* Privacy *europeo: commentario alla nuova disciplina sulla protezione dei dati personali, Milano, 2016,* 11.
[124] In tal senso si veda il Considerando 16 del GDPR.
[125] Cfr. Considerando 18.
[126] Cfr. Considerando 19.

retention,[127]in quanto istituto esclusivamente finalizzato all'immissione di dati aventi efficacia probatoria all'interno del procedimento penale[128].

Per quanto concerne la conservazione dei dati di traffico telefonico e telematico, il d. lgs. 10 agosto 2018, n. 101[129] ha novellato l'articolo 132 del Codice *Privacy,* modificando i commi 3 e 5 ed aggiungendo il comma 5-*bis*.

Di seguito, verrà effettuata una ricognizione della disciplina tuttora vigente, prestando particolare attenzione alle modifiche da ultimo introdotte dal legislatore.

4.1 Tipologia di dati e tempi di conservazione.

In base all'analisi condotta sin qui, risulta ormai acclarato che l'istituto della *data retention* sia scindibile in due fasi: il profilo della conservazione e quello dell'acquisizione dei dati di traffico[130]. Seppur distinti e destinatari di autonoma considerazione normativa, i due momenti sono correlati sul piano logico-strutturale, in

[127] L'istituto in esame rientra infatti nell'ambito di applicazione della direttiva (Ue) 2016/680 (Cfr. *nota* 83). In tal senso, si veda il Considerando 34 della direttiva sopracitata che dispone «Il trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, dovrebbe riguardare qualsiasi operazione o insieme di operazioni compiute nei confronti di dati personali o insiemi di dati personali per tali finalità, con l'ausilio di strumenti automatizzati o in altro modo, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, il raffronto o l'interconnessione, la limitazione del trattamento, la cancellazione o la distruzione…
… Se i dati personali sono stati inizialmente raccolti da un'autorità competente per una delle finalità della presente direttiva, il regolamento (UE) 2016/679 dovrebbe applicarsi al trattamento di tali dati per finalità diverse da quelle della presente direttiva, qualora detto trattamento sia autorizzato dal diritto dell'Unione o dello Stato membro. In particolare, le norme del regolamento (UE) 2016/679 dovrebbero applicarsi alla trasmissione di dati personali per finalità che non rientrano nell'ambito di applicazione della presente direttiva…». In dottrina v. BACCARI, *Il trattamento (anche elettronico) dei dati personali per finalità di accertamento dei reati*, in AA. VV., *Cybercrime,* (a cura di) CADOPPI, CANESTRARI, MANNA, PAPA, Torino, 2019, 1604.

[128] Nonostante la materia della c.d. *data retention* non ricada nell'ambito di applicazione del GDPR, nel corso del presente lavoro non mancheranno rinvii al suddetto regolamento. Questo rappresenta infatti un punto di riferimento costante in merito al trattamento dei dati personali.

[129] L'articolo 11 del d.lgs. n. 101/2018, rubricato «Modifiche alla parte II, titolo X, del d.lgs n. 196/2003», è intervenuto sulle disposizioni in materia di protezione dei dati personali nel settore delle comunicazioni elettroniche accessibili al pubblico.

[130] L'esistenza di due profili, di conservazione e di apprensione dei dati di traffico, entrambi ascrivibili all'istituto del *data retention* è confermata dalla CGUE, Gr. Sez., 21 Dicembre 2016, *Tele2 Sverige* AB c. Autorità svedese di Sorveglianza Poste e TLC, e Id., Gr. Sez., 8 aprile 2014, *Digital Rights Ireland e Seitlinger e altri*. Ancor prima era stata posta in rilievo dalla Corte costituzionale, nella sentenza 14 novembre 2006, n. 32, in *Giur. Cost*., 2006, p. 3916. Per un approfondimento sul contenuto della sentenza Cfr. Cap. II.

quanto il primo è condizione necessaria e sufficiente per la realizzazione del secondo[131].

L'autorità giudiziaria non potrebbe entrare in possesso dei dati telefonici e telematici a fini di indagine se gli stessi non fossero stati *ex ante* archiviati dai fornitori di servizi. La fase di conservazione è dunque preordinata a garantire la disponibilità dei suddetti per l'accertamento e il perseguimento dei reati e la loro eventuale apprensione nel corso del procedimento penale. A tale attività sono dedicati interamente i commi 1 e 1-*bis* dell'articolo 132 del Codice *privacy,* da ultimo modificati con la novella 109/2008[132].

La norma in esame si apre con un rinvio mobile all'articolo 123 del Codice *Privacy*, il cui primo comma prevede che i dati relativi al traffico riguardanti i contraenti e gli utenti trattati dal gestore sono cancellati o resi anonimi non appena cessino di essere utili ai fini del servizio reso. Tale assunto, preordinato a garantire la riservatezza e la segretezza delle comunicazioni, viene derogato in due casi distinti che non devono essere oggetto di confusione.

Nel primo caso, i "dati esterni" della comunicazione generati mediante il flusso telefonico e telematico possono essere conservati dal fornitore del servizio prescelto per esigenze di fatturazione[133] o di commercializzazione[134]. L'attività di archiviazione *de qua* è preordinata al soddisfacimento di interessi privati e non può protrarsi per più di sei mesi.

Il secondo caso di deroga rispetto all'assunto secondo cui i dati di traffico non possono subire alcun trattamento da parte di coloro che li detengono, è quello previsto dall'articolo 132. Come si è già visto ampiamente, tale norma del Codice *Privacy* prevede l'obbligo di archiviazione in capo ai fornitori dei servizi di comunicazione elettronica per esigenze di natura pubblicistica. In parallelo rispetto a quanto stabilito dall'art. 123 comma 2 e 3, la legge affida ai *provider* il compito di archiviare i medesimi dati in funzione ausiliaria rispetto alle autorità inquirenti. Si viene così a realizzare una forma di cooperazione tra il privato, *sub specie* i fornitori di servizi

[131] In tal senso ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, *cit.*, 82.
[132] V. *supra,* Cap. I § 3.5.
[133] Cfr. art. 123, comma 2.
[134] Cfr. art. 123, comma 3.

telefonici e telematici, e l'autorità giudiziaria per consentire l'esercizio di prerogative di natura processuale che altrimenti rimarrebbero insoddisfatte[135].

Nonostante entrambe le norme in esame prevedano un'ipotesi di conservazione dei dati "esterni" alla comunicazione, nel primo caso la fonte di legittimazione è di natura contrattuale, nel secondo i *provider* sono destinatari di un obbligo *ex lege*. Tale processo di registrazione del traffico di comunicazioni è automatizzato e viene effettuato nei confronti di tutti gli utenti. Prima di essere memorizzati in appositi tabulati, i dati sono elaborati mediante un processo di informatizzazione[136].

Sulla base di quanto appena esposto, emerge la complessità di interessi contrapposti che incidono sull'istituto della *data retention*. L'interferenza tra gli stessi attribuisce all'attività in esame una struttura triangolare[137].

Da una parte, si ha l'interesse primario dell'utente di subire un trattamento dei dati di traffico il più possibile limitato e circostanziato nel tempo. Specularmente opposta è invece l'esigenza dell'autorità giudiziaria di trattenere i dati in "lungo periodo" per garantirne il loro utilizzo per finalità di indagine. Infine, subentra l'interesse contabile del fornitore del servizio nel disporre l'archiviazione dei dati per fini *latu sensu* contrattuali ed estranei alla logica pubblicistica.

Quest'ultimo aspetto risulta indubbiamente secondario rispetto alla tutela della segretezza delle comunicazioni e all'interesse pubblico dell'accertamento e della repressione dei reati. Non è però del tutto irrilevante per il legislatore che garantisce anche le esigenze economiche dell'ente privato, seppur con intensità ridotta.

Per quanto concerne invece i tempi di conservazione[138], il primo comma dell'articolo 132 prevede ventiquattro mesi per i dati di traffico telefonico e dodici per il traffico telematico. Tale periodo decorre dalla data della comunicazione a cui si

---

[135] Le autorità inquirenti, infatti, non sarebbero in grado di provvedere in autonomia alla conservazione dei dati. In tal senso, l'attività di intermediazione dei *service provider* risulta inevitabile.

[136] MELILLO, *L'acquisizione dei tabulati relativi al traffico telefonico fra i limiti normativi ed equivoci giurisprudenziali*, in *Cass. Pen.*, 1999, 473.

[137] Sulla tridimensionalità del rapporto si veda MARCOLINI, *L'istituto della* data retention *dopo la sentenza della corte di giustizia del 2014, cit.,* 1583.

[138] Si ritiene utile riportare l'art 132, comma 1, attualmente in vigore:
«Fermo restando quanto previsto dall'*articolo 123, comma 2*, i dati relativi al traffico telefonico sono conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione di reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione.

riferiscono. Ai sensi del comma 1-*bis*[139] i dati relativi alle chiamate senza risposta[140] sono oggetto di attività di archiviazione per un periodo di gran lunga più breve, pari a trenta giorni. In riferimento a tale categoria autonoma di dati, non si specifica il termine a partire dal quale decorre il periodo di conservazione, che al primo comma coincide con la «data della comunicazione». Secondo un'interpretazione sistematica[141], il suddetto *dies a quo* può ritenersi coincidente con quello in cui il mittente instauri la connessione con l'utenza del destinatario, anche in assenza di una comunicazione.

Sorvolando su questioni meramente formali, occorre osservare che lo scaglionamento delle tempistiche attualmente in vigore solleva molteplici perplessità[142]. Innanzitutto, la scelta del legislatore di dimezzare il periodo di conservazione dei dati telematici rispetto a quelli telefonici risulta anacronistica in un'epoca in cui le comunicazioni elettroniche hanno preso il sopravvento su quelle tradizionali[143].

Più coerente e in linea con la tipologia di servizi di comunicazione maggiormente diffusa tra gli utenti, sarebbe stata la scelta di invertire i periodi predeterminati, concedendo tempi di archiviazione maggiore ai tabulati relativi al flusso informatico. Ancora più irragionevole risulta il periodo previsto per le chiamate senza risposta. Non si comprende infatti come sia possibile soddisfare le esigenze

[139]L'art. 132, comma 1-*bis*, dispone che «I dati relativi alle chiamate senza risposta, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione, sono conservati per trenta giorni».

[140] Ai sensi dell'articolo 1, lett *e)* del d.lgs. 109/2008 con «chiamata senza risposta» si intende «la connessione istituita da un servizio telefonico accessibile al pubblico, non seguita da un'effettiva comunicazione, in quanto il destinatario non ha risposto ovvero vi è stato un intervento del gestore della rete». Tale definizione richiama quella fornita dall'art. 2, comma 2, lett. *f)* della direttiva 2006/24/CE secondo cui «il tentativo di chiamata non riuscito» consiste in «una chiamata telefonica che è stata collegata con successo ma non ha ottenuto risposta, oppure in cui vi è stato un intervento del gestore della rete».

[141] Sul punto si veda ATERNO, *Conservazione dei dati informatici e prospettive europee, cit.,* 165; nello stesso senso ATERNO, CISTERNA, *Il legislatore interviene ancora sulla* data retention*, ma non è finita*., in *Dir. Pen. e proc*., 2009, 279.

[142] In tal senso SIGNORATO, *Novità in tema di* data retention*. La riformulazione dell'art. 132 codice privacy da parte del D. Lgs. 10 agosto 2018 n. 101*, in *Dir. Pen. contemp.*, 2018, 156; IDEM, *Contrasto al terrorismo e* data retention: *molte ombre e poche luci*, in KOSTORIS-VIGANO' (a cura di), *Il nuovo pacchetto antiterrorismo*, Torino, 2015, 80.

[143] Si veda RAFARACI, *Intercettazioni e acquisizioni di tabulati telefonici*, in KOSTORIS – ORLANDI (a cura di), *Contrasto al terrorismo interno e internazionale,* Torino, 2006, 276. L'Autore sottolinea come la *ratio* originaria della differenziazione dei tempi di archiviazione fosse quella di ridurre i costi legati alla conservazione dei dati, molto più alti in caso di archiviazione di dati telematici.

investigative, anche soltanto quelle relative all'acquisizione della notizia di reato, in soli trenta giorni[144].

Al contrario, il periodo di conservazione così ridotto rischia di comportare la perdita di informazioni essenziali specialmente nell'ambito di indagini aventi ad oggetto reati in materia di terrorismo. Si pensi al caso in cui la «chiamata senza di risposta», o in tono più colloquiale lo "squillo", costituisca il segnale per la detonazione di un esplosivo. È inverosimile ritenere l'autorità giudiziaria in grado di iniziare l'indagine e perfezionare l'acquisizione dei dati di traffico entro trenta giorni dalla realizzazione della chiamata[145].

Ne consegue che la disciplina previgente[146] secondo cui le chiamate senza risposta erano ricomprese nella più generale categoria dei dati di traffico telefonico, risultava di gran lunga più ragionevole. Inoltre, la scelta di dettare tempistiche differenziate appare ancora più incoerente se si considera che non trova giustificazione in una maggiore incidenza sui diritti fondamentali dei dati esterni relativi alle chiamate senza risposta.

Al di là della discutibile determinazione dei tempi di conservazione, è opportuno precisare che questi risultano fissi e in nessun modo calibrati sulla tipologia di delitti per cui si procede. Il legislatore si limita a differenziare le tempistiche in base alla provenienza dei dati, a seconda che siano generati dalle comunicazioni via telefono o tramite rete Internet.

Non fa invece alcun riferimento né agli utenti di cui i dati siano passibili di archiviazione né alle fattispecie penali per cui è possibile procedere. La prospettiva teleologica relativa alle «finalità di accertamento e repressione dei reati»[147]risulta così ampia e generica da ricomprendere l'attività di indagine avente ad oggetto qualsiasi tipologia criminosa, indipendentemente dalla sua gravità. Sul piano oggettivo, l'autorità giudiziaria può disporre l'acquisizione dei dati di traffico sia in funzione

[144] È opportuno osservare che il suddetto termine di conservazione relativo alle chiamate senza risposta, è addirittura più basso della soglia minima di sei mesi stabilita nella "direttiva Frattini". Eppure, ai sensi dell'articolo 3 comma 2 si stabiliva espressamente che la disciplina della *data retention* includeva dati relativi alle chiamate senza risposta.
[145] Sul punto CONTI, *L'attuazione della direttiva Frattini*, *cit.*, 18.
[146] Si fa qui riferimento al decreto-legge 144/2005 che aveva espressamente ricompreso le chiamate senza risposta nell'ambito dei dati di traffico telefonico. Cfr. Cap I § 3.3.
[147] Cfr. art 132, comma 1.

dell'accertamento dei c.d. "serious crimes" (criminalità organizzata, pedopornografia, terrorismo etc. etc.) sia in caso di contravvenzioni di scarsa rilevanza penale.

Ebbene, il *deficit* di determinatezza riguardo alle tipologie di reati per cui è possibile accedere ai dati di traffico costituisce un essenziale *puctum dolens* della disciplina attualmente vigente[148].

Ciò posto, è necessario proseguire con l'esegesi dell'art. 132 del Codice *privacy*. Una volta prescritto l'obbligo di archiviazione in capo ai fornitori, la norma non si dilunga ulteriormente né su cosa intenda per «dati relativi al traffico» né su quali siano le categorie di dati ascrivibili in concreto a tale categoria. Tali lacune dal punto di vista definitorio concorrono a minare l'autosufficienza del Codice *privac*y, in quanto possono essere colmate soltanto mediante il rinvio a atti normativi esterni.

Sul punto, in seguito all'abrogazione dell'art. 4 comma 2 lett. h)[149] del d.lgs. 196/2003, è d'ausilio l'art. 3[150] del d.lgs. 109/2008 rubricato «Categorie di dati da

---

[148] ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, *cit.*,97.

[149] Come si è accennato, ai sensi dell'art. 4 comma 2 lett. h) del Codice *Privacy* la definizione dei dati relativi al traffico era così formulata «qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione». Tale norma è stata abrogata con il d.lgs. 101/2018.

[150] Per ragioni di completezza si riporta di seguito l'art. 3, comma 1 del d.lgs. 109/2008:
«1. Le categorie di dati da conservare per le finalità di cui all'articolo 132 del Codice sono le seguenti:
a) i dati necessari per rintracciare e identificare la fonte di una comunicazione:
1) per la telefonia di rete fissa e la telefonia mobile:
1.1 numero telefonico chiamante;
1.2 nome e indirizzo dell'abbonato o dell'utente registrato;
2) per l'accesso internet:
2.1 nome e indirizzo dell'abbonato o dell'utente registrato a cui al momento della comunicazione sono stati univocamente assegnati l'indirizzo di protocollo internet (IP), un identificativo di utente o un numero telefonico;
3) per la posta elettronica:
3.1 indirizzo IP utilizzato e indirizzo di posta elettronica ed eventuale ulteriore identificativo del mittente;
3.2 indirizzo IP e nome a dominio pienamente qualificato del mail *exchanger host*, nel caso della tecnologia SMTP ovvero di qualsiasi tipologia di *host* relativo ad una diversa tecnologia utilizzata per la trasmissione della comunicazione;
4) per la telefonia, invio di fax, sms e mms via internet:
4.1 indirizzo IP, numero telefonico ed eventuale altro identificativo dell'utente chiamante;
4.2 dati anagrafici dell'utente registrato che ha effettuato la comunicazione;
b) i dati necessari per rintracciare e identificare la destinazione di una comunicazione:
1) per la telefonia di rete fissa e la telefonia mobile:
1.1 numero composto, ovvero il numero o i numeri chiamati e, nei casi che comportano servizi supplementari come l'inoltro o il trasferimento di chiamata, il numero o i numeri a cui la chiamata e' trasmessa;
1.2 nome e indirizzo dell'abbonato o dell'utente registrato;
2) per la posta elettronica:
2.1 indirizzo di posta elettronica, ed eventuale ulteriore identificativo, del destinatario della

conservare per gli operatori di telefonia e di comunicazione elettronica». Tale norma ripropone quasi alla lettera il contenuto dell'articolo 5 della direttiva Frattini[151] e

comunicazione;
2.2 indirizzo IP e nome a dominio pienamente qualificato del mail *exchanger host* (nel caso della tecnologia SMTP), ovvero di qualsiasi tipologia di *host* (relativamente ad una diversa tecnologia utilizzata), che ha provveduto alla consegna del messaggio;
2.3 indirizzo IP utilizzato per la ricezione ovvero la consultazione dei messaggi di posta elettronica da parte del destinatario indipendentemente dalla tecnologia o dal protocollo utilizzato;
3) telefonia, invio di fax, sms e mms via internet:
3.1 indirizzo IP, numero telefonico ed eventuale altro identificativo dell'utente chiamato;
3.2 dati anagrafici dell'utente registrato che ha ricevuto la comunicazione;
3.3 numero o numeri a cui la chiamata e' trasmessa, nei casi di servizi supplementari come l'inoltro o il trasferimento di chiamata;
c) i dati necessari per determinare la data, l'ora e la durata di una comunicazione:
1) per la telefonia di rete fissa e la telefonia mobile, data e ora dell'inizio e della fine della comunicazione;
2) per l'accesso internet :
2.1 data e ora (GMT) della connessione e della disconnessione dell'utente del servizio di accesso internet, unitamente all'indirizzo IP, dinamico o statico, univocamente assegnato dal fornitore di accesso internet a una comunicazione e l'identificativo dell'abbonato o dell'utente registrato;
3) per la posta elettronica:
3.1 data e ora (GMT) della connessione e della disconnessione dell'utente del servizio di posta elettronica su internet ed indirizzo IP utilizzato, indipendentemente dalla tecnologia e dal protocollo impiegato;
4) per la telefonia, invio di fax, sms e mms via internet:
4.1 data e ora (GMT) della connessione e della disconnessione dell'utente del servizio utilizzato su internet ed indirizzo IP impiegato, indipendentemente dalla tecnologia e dal protocollo usato;
d) i dati necessari per determinare il tipo di comunicazione:
1) per la telefonia di rete fissa e la telefonia mobile: il servizio telefonico utilizzato;
2) per la posta elettronica internet e la telefonia internet: il servizio internet utilizzato;
e) i dati necessari per determinare le attrezzature di comunicazione degli utenti o quello che si presume essere le loro attrezzature:
1) per la telefonia di rete fissa, numeri telefonici chiamanti e chiamati;
2) per la telefonia mobile:
2.1 numeri telefonici chiamanti e chiamati;
2.2 *International Mobile Subscriber Identity* (IMSI) del chiamante;
2.3 *International Mobile Equipment Identity* (IMEI) del chiamante;
2.4 l'IMSI del chiamato;
2.5 l'IMEI del chiamato;
2.6 nel caso dei servizi prepagati anonimi, la data e l'ora dell'attivazione iniziale della carta e l'etichetta di ubicazione (*Cell* ID) dalla quale e' stata effettuata l'attivazione;
3) per l'accesso internet e telefonia, invio di fax, sms e mms via internet:
3.1 numero telefonico chiamante per l'accesso commutato (*dial-up access*);
3.2 *digital subscriber line number* (DSL) o un altro identificatore finale di chi e' all'origine della comunicazione;
f) i dati necessari per determinare l'ubicazione delle apparecchiature di comunicazione mobile:
1) etichetta di ubicazione (Cell ID) all'inizio della comunicazione;
2) dati per identificare l'ubicazione geografica della cella facendo riferimento alle loro etichette di ubicazione (Cell ID) nel periodo in cui vengono conservati i dati sulle comunicazioni.»

[151] Nonostante la direttiva non sia più in vigore a seguito della sentenza *Digital Rights Ireland Ltd*, l'articolo 5 della stessa continua ad essere un punto di riferimento per la determinazione delle categorie di dati di traffico.

fornisce un elenco tassativo dei dati rientranti nella categoria di «dati relativi al traffico»[152], a loro volta distinti in sei sottocategorie.

Fanno parte della prima e della seconda i dati che permettono l'individuazione rispettivamente del mittente e del destinatario della comunicazione. Sono inclusi il numero telefonico dell'utente qualora la conversazione sia istaurata mediante l'accesso a rete telefonica; l'indirizzo IP nel caso in cui si tratti di un flusso telematico mediante posta elettronica o messaggistica via Internet. Alla terza categoria appartengono i dati che identificano la data, l'ora e la durata della comunicazione o, nel caso di accesso alla rete, della connessione e della disconnessione dell'utente al servizio telematico prescelto. Seguono poi quelli che permettono di determinare il tipo di conversazione instaurata e gli strumenti telefonici o telematici utilizzati dagli utenti, inclusa l'ubicazione degli strumenti di comunicazione.

Come si è accennato poco sopra, tale elenco deve intendersi un catalogo chiuso[153]. Pertanto, le tipologie di dati non rientranti nelle categorie sopraindicate, ad esempio i nomi dei siti visitati da un determinato utente, devono considerarsi non passibili di conservazione e acquisizione per finalità di accertamento e repressione dei reati[154]. Ciò posto, i dati di traffico esclusi dal novero appena enucleato sono in numero assai ridotto.

In sintesi, il regime previsto dall'articolo 132 comprende tutti i dati di traffico e di ubicazione generati con qualsiasi mezzo di comunicazione elettronica (telefono cellulare, Internet, posta elettronica etc etc.) da parte di qualsiasi utente abbonato e registrato. Tale attività sistematica realizza dunque una raccolta generalizzata di "tutto di tutti"[155], essendo sufficiente il collegamento ad una qualsiasi attività di comunicazione elettronica. In assenza di parametri oggettivi che limitino la portata

---

[152] Sul punto si veda il Provvedimento del Garante della *Privacy* del 17 Gennaio 2008 "Sicurezza dei dati di Traffico telefonico e telematico", in *Guida dir*., 2008, n. 9, 88.

[153] In tal senso CONTI, *L'attuazione della direttiva Frattini*, *cit.*, 15. Secondo l'Autrice, la disciplina della c.d. *data retention*, prevedendo una vistosa deroga alla tutela del bene costituzionale della segretezza delle comunicazioni garantita dall'articolo 15 Cost., non può che essere oggetto di un'interpretazione all'insegna del principio di tassatività. Nello stesso senso, BUSIA, *Elenco tassativo delle informazioni da archiviare*, in *Guida dir*., 2004, n. 2, 29; al contrario, in senso favorevole all'ampliamento del catalogo dei dati acquisibili AMATO, *Il reato grave facilita l'accesso al tabulato*, *cit.*, 31.

[154] Il punto verrà approfondito in seguito Cfr. Cap II.

[155] L'espressione è di FATTA, *La tutela della* privacy *alla prova dell'obbligo di* data retention *e delle misure antiterrorismo*, in *Dir. dell'informatica e dell'informazione*, 2008, 408.

della disciplina in esame, sono davvero pochi i dati che non rientrano nel relativo ambito di applicazione.

Tali informazioni, caratterizzate da una valenza divulgativa su elementi sulla personalità e la vita privata dell'intestatario dell'utenza telefonica[156], sono connotate da un'elevata rilevanza probatoria. Ai fini della loro acquisizione all'interno del procedimento penale vengono incorporate in un prodotto fisico che ha natura documentale. Questo è comunemente noto con nome di tabulato telefonico o anche *Call Detail Records* (in acronimo CDR)[157]. Si tratta di un supporto cartaceo o digitale[158] (cd, chiavetta USB etc. etc.) in cui sono registrate i dati di traffico telefonico e telematico di utenza mobile o fissa in un determinato arco di temporale.

Tale prospetto viene realizzato dai fornitori dei servizi di comunicazione elettronica che si trovano automaticamente in possesso di tali informazioni. Si tratta dunque di una prova precostituita in quanto formata al di fuori del procedimento ed esistente indipendentemente dall'avvio di un'inchiesta penale[159].

4.2 I gestori di servizi telefonici e telematici.

Dopo aver fornito le coordinate relative alla tipologia di dati e all'attività di archiviazione svolta dai gestori di servizi di comunicazione elettronica, è necessario fornire una definizione di gestori di servizi di comunicazione per capire in capo a chi, di fatto, incomba l'obbligo di archiviazione.

Si tratta solitamente di enti o società private che mettono a disposizione servizi a pagamento consistenti nella trasmissione di segnali su reti di comunicazioni

---

[156] Cfr. BUSIA, *Così la riservatezza "guadagna" terreno*, in *Guida dir.*, 2004, n. 10, 58. L'Autore afferma che «non è vero che il trattamento dei dati sul traffico sia per sé innocuo o comunque meno meritevole di tutela rispetto al contenuto delle comunicazioni cui gli stessi si riferiscono. Anche tali informazioni, solo apparentemente "esteriori", sono infatti in grado di rivelare la rete delle relazioni personali e sociali di un individuo». Nello stesso senso, FRIGO, *Nella conservazione dei dati internet la necessaria tutela giurisdizionale*, *cit.*, 14.

[157] Tale acronimo viene comunemente tradotto in italiano con l'espressione "cartellino di traffico".

[158] La modalità prescelta di incorporamento dei dati storici identificativi i flussi di chiamate, non muta l'attitudine rappresentativa della *res* e dunque la rilevanza probatoria delle informazioni in essa custodite.

[159] Cfr. ZICCARDI, *Aspetti informatici giuridici della fonte di prova digitale*, in LUPÀRIA, ZICCARDI, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, 2007, 249.

elettroniche accessibili al pubblico[160]. A tale ampia categoria appartengono i fornitori di servizi di telefonici e telematici. I primi, dietro la stipula di un contratto di fornitura, garantiscono la ricezione o la trasmissione di informazioni tra più utenti attraverso l'accesso ad una rete di telecomunicazione. Sono annoverati tra i servizi "telefonici": le chiamate telefoniche, incluse quelle vocali, di messaggeria vocale, in conferenza e di trasmissione dati tramite *telefax*; i servizi supplementari, inclusi l'inoltro e il trasferimento in chiamata; la messaggeria e i servizi multimediali, inclusi i servizi di messaggeria breve o *sms*.

Invece, i fornitori di servizi telematici o c.d. *internet service provider* consentono agli utenti la comunicazione mediante un sistema informatico ovvero processano e archiviano dati informatici per conto di tale servizio di comunicazione o per utenti dello stesso[161].

Vengono, inoltre, distinti in tre sottocategorie a seconda che svolgano rispettivamente attività di *mere conduit*, di *caching* e di *hosting*[162], e cioè trasmettano informazioni non proprie date dal destinatario del servizio, realizzino attività di memorizzazione temporanea (ad esempio attraverso la creazione di *mailing list* o *newsgroup*) ovvero garantiscano semplicemente accesso alla Rete. Sono inclusi tra i servizi "telematici" forniti dagli *internet service provider*: l'accesso alla rete *Internet*, la posta elettronica, i *fax* e gli *Over the top media service* (in acronimo OTT),[163]tra cui la telefonia via *Internet* o *VoIP* (*Voice over Internet Protocol)*[164].

---

[160] Per una definizione di «reti di comunicazione elettronica» si veda l'art. 4 del Codice *Privacy*, ormai abrogato. Tra gli atti legislativi comunitari, è opportuno rinviare alla Direttiva quadro 2002/21/CE del Parlamento europeo e del Consiglio «che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica».

[161] Per una definizione di *Internet service provider* si veda l'articolo 1 lett. c) della Convenzione di Budapest.

[162] In tal senso, PICOTTI, *Diritto penale e tecnologie informatiche: una visione di insieme,* in AA. VV., *Cybercrime,* a cura di CADOPPI, CANESTRARI, MANNA, PAPA,Torino, 2019, 33.

[163] *Over-the-top* è la categoria di servizi di comunicazione di audio, video e altri media su Internet senza il coinvolgimento dell'operatore di rete nel controllo o distribuzione del contenuto (vedi ad esempio *WhatsApp, Facebook, Messenger*, *Skype, Microsoft teams* per operazioni di messaggistica e VOIP; servizi di video-streaming, come *Netflix, Amazon Prime, YouTube*). Negli ultimi anni, questi e molti altri tendono a sostituire sempre di più la tradizionale telefonia vocale e SMS con servizi *online* funzionalmente equivalenti. Per un approfondimento sul punto si veda CAGGIANO, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione,* in *Medialaws – Rivista dir. media*, 2018, n. 2, 72.

[164] Con *VOIP* si fa riferimento ad una tipologia di servizi OTT (vedi nota precedente) che consente di far transitare la voce in uscita e in ingresso sfruttando la connessione ad internet o una rete che utilizzi il protocollo IP invece di utilizzare la rete telefonica tradizionale (PSTN). Sulla questione interpretativa riguardante la possibilità di estendere la procedura prevista per l'acquisizione e la conservazione dei tabulati alle chiamate effettuate con i sistemi di VOIP si veda BUSETTO, *La Commissione Europea torna*

Seppur utile ad un maggiore inquadramento dogmatico, è opportuno precisare che, negli ultimi anni, la suddivisione dei *provider* nelle macro-categorie sopradescritte dei gestori di servizi telefonici e telematici è stata superata. Spesso, infatti, vengono offerti agli utenti un cumulo di prestazioni professionali comprensive di entrambe le funzioni.

4.3 Il procedimento acquisitivo dei dati da parte dell'autorità giudiziaria.

Dopo aver disciplinato l'attività e i tempi di archiviazione dei dati di traffico, l'articolo 132 prosegue regolando le modalità acquisitive degli stessi all'interno del procedimento penale. L'impianto originario del comma 3, da ultimo modificato con il d.lgs. 108/109, è rimasto pressoché invariato in quanto la novella del 2018 si è limitata ad introdurre soltanto degli elementi di coordinamento alla normativa preesistente[165].

La disciplina risultante, prevede che i dati possono essere acquisiti con decreto motivato dal pubblico ministero, d'ufficio o su istanza del difensore dell'imputato o delle altre parti private. Mediante tale previsione, il legislatore realizza una *reductio ad unum* dell'*iter* di acquisizione che viene interamente affidata alla pubblica accusa. Tale accentramento sostituisce il previgente riparto di competenze tra pubblico ministero e giudice[166].

Sul piano dell'accessibilità ai dati di traffico si abbandona dunque la logica del "doppio binario" secondo cui la procedura di acquisizione veniva modulata in base alla gravità del reato per cui si procedeva o in base al periodo di conservazione. Siffatta graduazione della tutela della segretezza delle comunicazioni, in correlazione alla durata del periodo di conservazione, viene ora sostituita da una procedura semplificata e monofasica.

Per quanto riguarda invece i presupposti oggettivi legittimanti l'accessibilità dei dati il regime attuale si contraddistingue negativamente per un'ampia lacuna

---

ad occuparsi del mercato unico digitale: una prima analisi della proposta del nuovo regolamento in tema di comunicazioni elettroniche, consultabile *online* su *www.filodiritto.it*.

[165] L'art. 132, comma 3, prevede che «Entro il termine di cui al comma 1, i dati sono acquisiti presso il fornitore con decreto motivato del pubblico ministero anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private…»

[166] Si fa riferimento alle precedenti versioni dell'articolo 132 del codice Privacy come modificate dal d.l. 354/2003 e dalla l. 45/2004. Per un maggiore approfondimento si rimanda a quanto detto *supra* Cap I § 3. e 3.2.

normativa.[167] Il terzo comma dell'articolo 132 si limita infatti a prevedere che «entro il termine di cui al comma 1», i dati sono acquisibili presso il fornitore di servizi mediante decreto motivato del P.M.

L'unico parametro oggettivo è desumibile sul piano esegetico dalla prospettiva teleologica contenuta nel primo comma dell'articolo 132 e implicitamente richiamata nel comma 3. Se l'istituto della c.d. *data retention* risponde a «finalità di accertamento e di repressione dei reati» i dati di traffico da acquisire devono presentare un nesso con il reato oggetto di indagini. In linea con tale interpretazione, affinché l'autorità giudiziaria possa acquisire i tabulati telefoni e telematici dai fornitori, è necessaria la presenza di elementi conoscitivi idonei a far ritenere sussistente un illecito penale.

La norma non specifica però quali elementi devono intendersi come sintomatici di un collegamento tra una determinata utenza telefonica ed un illecito penale di cui è pervenuta *notitia criminis*. In dottrina, ci si è interrogati se siano sufficienti dei "meri indizi" da cui si può induttivamente dedurre l'esistenza di un fatto ignoto da provare o se sia necessario che questi siano connotati da un grado più elevato di intensità conoscitiva.

Secondo tale lettura più garantista, sarebbe necessario subordinare l'attività di acquisizione alla sussistenza del *fumus commissi delicti* che attesti l'esistenza di un grave indizio di colpevolezza. Tale elemento probatorio inequivoco eviterebbe una raccolta arbitraria ed indiscriminata dei dati di traffico lesiva dei diritti personali dell'individuo[168].

Un altro *vacuum* della disposizione in esame riguarda l'assenza di limiti soggettivi entro i quali l'autorità giudiziaria può procedere a tale attività di indagine. La norma non si esprime in merito alla sussistenza di un nesso tra l'apparecchio elettronico (telefono o computer) da controllare e l'ipotesi di reato oggetto di indagine.

In mancanza di una chiara disposizione in tal senso, l'apprensione può riguardare non solo i dati di traffico relativi ad utenze telefoniche o telematiche della persona sottoposta alle indagini o imputata[169], ma anche a quelle intestate a soggetti

---

[167] ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, *cit.*, 2018, 98.

[168] Sul punto, CAIANIELLO, *Il principio di proporzionalità nel processo penale,* in *Diritto penale contemporaneo – Rivista trimestrale*, 2014, 143 ss.

[169] In senso analogo si è espressa la dottrina maggioritaria in materia di intercettazioni. A favore della tesi che ammette l'attività di captazione delle comunicazioni nei confronti di soggetti non sottoposti ad

estranei alla commissione del reato per cui si procede, in presenza di elementi concreti per far ritenere che queste siano utilizzate dall'indagato o siano comunque attinenti al *factum criminis de quo*.

La decisione del legislatore di non circoscrivere dal punto di vista soggettivo l'accessibilità dei dati, consente alle autorità inquirenti di ricorrere all'istituto del *data retention* anche nei procedimenti a carico di ignoti, laddove non sia identificato il soggetto indagato. Rende possibile, inoltre, l'intercettazione di quei comportamenti elusivi, come l'utilizzo di un telefono di un conoscente, che non sarebbero altrimenti individuabili mediante il controllo esclusivamente diretto all'imputato.

Se, da una parte, tale estensione soggettiva garantisce un'efficienza investigativa non irrilevante, dall'altra porta con sé il rischio di un utilizzo arbitrario ed eccessivamente invasivo dello strumento di *data retention*. Non è da sottovalutare la possibilità che l'attività di apprensione dei tabulati, proprio perché sciolta da qualsiasi vincolo di natura soggettiva, possa trasformarsi da mezzo di ricerca della prova a strumento "esplorativo" finalizzato all'acquisizione della notizia di reato[170].

Inoltre, l'indeterminatezza nell'individuazione dei presupposti oggettivi e soggettivi per procedere all'acquisizione dei dati determina un atteggiamento di minor rigore nell'adempimento dell'obbligo motivazionale del P.M.

Come si è anticipato, il terzo comma dell'articolo 132 del Codice *Privacy* prevede un obbligo di esposizione delle ragioni che giustificano l'esercizio del potere di apprensione dei dati di traffico. Tale disposizione trova fondamento nell'art. 15 comma 2, Cost. che prevede una riserva di giurisdizione ogniqualvolta si incida sul diritto inviolabile della segretezza delle comunicazioni.

Sicché, nel caso di specie, l'autorità procedente dovrebbe dar conto dell'*iter* cognitivo e valutativo da essa seguito prima di procedere all'apprensione dei tabulati. La motivazione dovrebbe indicare il titolo del reato per cui si procede e gli elementi di prova che attestano che si sia verificato. Non dovrebbe inoltre omettere di

indagini v. CAMON, *Le intercettazioni nel processo penale*, Milano, 1996, 121; APRILE-SPEZIA, Le intercettazioni telefoniche ed ambientali. Innovazioni tecnologiche e nuove questioni giuridiche, Milano, 2004, 7-8; MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Torino, 2007, 43.

[170] Sul punto si veda ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, *cit.*, 104.

menzionare espressamente le esigenze investigative che in concreto si intendono soddisfare e la relazione di pertinenza tra la fattispecie criminosa e i dati acquisiti.

Nella prassi, però, l'assenza di un'espressa previsione sul contenuto della motivazione legittima una serie comportamenti distorsivi: frequentemente i decreti contengono motivazioni tautologiche o meramente apparenti[171]. Ancora più di frequente l'autorità competente si limita a riprodurre semplici clausole di stile o enunciazioni apodittiche che non riportano le reali ragioni a fondamento del provvedimento.

4.4 L'acquisizione dei tabulati di traffico telefonico su richiesta del difensore.

Fin qui, si è esaminato l'*iter* di apprensione da parte del pubblico ministero, detentore principale ma non esclusivo del potere di acquisizione dei dati. Ai sensi dell'art. 132, comma 3, infatti il difensore dell'imputato o di persona sottoposta alle indagini ha la possibilità di rivolgersi direttamente al gestore del servizio di comunicazione per l'acquisizione dei dati di traffico relativi al proprio assistito.

Tale previsione, già presente nelle versioni antecedenti[172] a quella attuale, risulta in linea con la rottura del monopolio del pubblico ministero nella fase delle indagini preliminari realizzata mediante l'inserimento della disciplina delle investigazioni difensive all'interno del codice di procedura penale[173]. Il legislatore ha disposto non solo che il privato "interessato" possa sollecitare, tramite il proprio difensore, l'operazione acquisitiva da parte del P.M. ma anche che abbia la possibilità provvedervi *motu proprio*. Atteso che la pubblica accusa non è obbligata ad acquisire i dati laddove riceva istanza da parte del difensore dell'indagato, il legislatore sopperisce all'eventuale inottemperanza dell'autorità giudiziaria conferendo un potere autonomo al patrocinatore.

---

[171] Sul punto ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, *cit.*, 113. In giurisprudenza, il Giudice di legittimità si è però espresso a favore dell'utilizzabilità dei tabulati telefonici anche in assenza di un provvedimento motivato da parte dell'autorità giudiziaria. Cfr. Cass. Pen., Sez. VI, 14 gennaio 2011, n. 8353, Formaggio, in *Cass. Pen*. 2012, 1813; Cass. Pen., Sez. IV, 24 febbraio 2005, n.20558, Pietroleonardo, in CED n. 231920.

[172] Si fa qui riferimento alle versioni risultanti dal d.l. 144/2005. Cfr. Cap §3.3.

[173] Si fa riferimento agli artt. 391-*bis* – 391-*decies* inseriti all'interno del Titolo VI *bis* dalla legge 7 dicembre 2000, n. 7. La regolamentazione delle investigazioni difensive da parte del legislatore italiano ha dato espresso riconoscimento al "principio di parità delle parti" all'interno del processo penale (art. 24 Cost, comma 2). Sul punto v. TONINI, *Manuale di procedura penale*, *cit.*, 666.

In ossequio a tale meccanismo, il difensore può disporre l'acquisizione dei tabulati inerenti alle utenze intestate al proprio assistito[174], secondo le modalità previste all'articolo 391-*quater*[175] del codice di procedura penale. Tale iniziativa istruttoria presenta un regime differenziato a seconda che la stessa riguardi l'acquisizione del «traffico in uscita»[176] o il «traffico in entrata»[177].

Nel primo caso, la richiesta del difensore deve essere corredata soltanto dall'atto di conferimento dell'incarico professionale, che attesti la legittimazione ad agire del difensore qualificato ai sensi dell'articolo 391-*quater*. Nel secondo caso, invece, è possibile proporre istanza di acquisizione ai tabulati soltanto qualora il mancato accesso agli stessi determinerebbe un «pregiudizio effettivo» alle indagini difensive. Oltre all'atto di conferimento dell'incarico, il difensore è dunque tenuto ad allegare elementi idonei a provare il suddetto «pregiudizio». Tali presupposti oggettivi sono stati individuati dal Garante della *Privacy* con il provvedimento del 3 novembre 2005[178].

All'interno di tale atto, si precisa che l'acquisizione dei dati personali rappresenta un'eccezione al principio generale per cui la conoscibilità dei dati di traffico è negata a terzi. Da tale assunto deriva che l'accesso è consentito soltanto laddove sia funzionale all'esplicazione del diritto di difesa, costituzionalmente garantito[179]. A tal fine, il difensore che dispone l'acquisizione dei dati in entrata deve

---

[174] Ai sensi dell'art. 132, comma 3, è previsto che «Il difensore dell'imputato o della persona sottoposta alle indagini può richiedere, direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'articolo 391-*quater* del codice di procedura penale. La richiesta di accesso diretto alle comunicazioni telefoniche in entrata può essere effettuata solo quando possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla *legge 7 dicembre 2000, n. 397*…».

[175] L'articolo 391-*quater,* rubricato «Richiesta di documentazione alla pubblica amministrazione» prevede che:

« Ai fini delle indagini difensive, il difensore può chiedere i documenti in possesso della pubblica amministrazione e di estrarne copia a sue spese. (comma 1)

L'istanza deve essere rivolta all'amministrazione che ha formato il documento o lo detiene stabilmente. (comma 2)

In caso di rifiuto da parte della pubblica amministrazione si applicano le disposizioni degli articoli 367 e 368. (comma 3)».

[176] Con tale espressione si fa riferimento ai dati relativi alle chiamate in partenza.

[177] Con tale espressione si fa riferimento ai dati relativi alle chiamate in arrivo.

[178] In *www.garanteprivacy.it*, doc. Web n. 1189488.

[179] La versione precedente stabiliva che l'acquisizione dei dati relativi alle chiamate in arrivo potesse avvenire ad opera del difensore dell'imputato «ferme restando le condizioni di cui all'art. 8, comma 2, lettera f, per il traffico entrante» (norma che fissa la necessità di dimostrare che la richiesta dei dati sia volta a prevenire il verificarsi di un pregiudizio effettivo e concreto per le indagini difensive). Opportunamente, la riforma semplifica la lettura della norma. Essa elimina il riferimento all'art. 8,

indicare «l'intenzione di utilizzare i dati esclusivamente nell'ambito del procedimento penale» in quanto è insufficiente che questi siano «semplicemente utili o funzionali al diritto di difesa»[180].

Seppur non sia indispensabile specificare il numero del procedimento penale[181], è necessario allegare una descrizione analitica e puntuale delle circostanze del fatto di reato su cui vertono le indagini difensive. Inoltre, il difensore è tenuto a dimostrare la necessità dell'accesso, dimostrando con idonei elementi probatori che dal diniego discenderebbe un pregiudizio effettivo e concreto per l'andamento delle indagini difensive. Infine, è opportuno aggiungere una dichiarazione mediante la quale si attesti la veridicità del contenuto di tutti gli atti presentati.

La sussistenza di tutti i requisiti suesposti viene accertata dal fornitore dei servizi elettronici destinatario dell'istanza in base alla documentazione allegata[182]. In particolare, il fornitore è tenuto a verificare l'esistenza del «pregiudizio effettivo» e la pertinenza dei dati richiesti rispetto al reato per cui si procede. Decorsi quindici giorni, trenta nei casi di maggiore complessità, dalla ricezione dell'istanza di accesso, il gestore dei servizi fornisce un riscontro all'interessato richiedente. Mediante una valutazione sulla sussistenza o meno di presupposti oggettivi, procederà ad autorizzare o a negare la conoscibilità dei dati. Viene così a sostanziarsi in capo all'ente privato una funzione "filtro"[183] preposta a verificare la legittimità delle richieste di accesso dei dati.

Ebbene, la configurazione in capo ad un soggetto del tutto estraneo al processo di un simile potere risulta assai critico. Secondo un'impostazione maggiormente coerente con l'attuale sistema penale, spetterebbe infatti al giudice esercitare un vaglio sulla legittimità di una operazione incidente sul diritto alla difesa delle parti[184]. Al contrario, la disciplina attuale prevede il subentro dell'autorità giudiziaria soltanto qualora il gestore risulti inadempiente. In tal caso, il difensore può rivolgersi

---

comma 2, lettera f, sostituendolo con la previsione sopracitata. Per un maggiore approfondimento v. SIGNORATO, *Novità in tema di* data retention, *cit.*, 158.

[180] Cfr. Garante della *Privacy*, Provvedimento del 3 novembre 2005. Vedi *supra*.

[181] Ciò in conformità con quanto previsto all'art. 391- *nonies* c.p.p. secondo cui le indagini difensive possono essere avviate lecitamente prima del procedimento penale e nell'eventualità che questa sia instaurato.

[182] CONTI, *L'attuazione della direttiva Frattini*, *cit.*, 28.

[183] Tale espressione è utilizzata da CONTI, *L'attuazione della direttiva Frattini*, *cit.*, 28.

[184] Il diritto alla difesa delle parti è un principio inviolabile di rango costituzionale previsto dall'art 24 Cost.

direttamente al pubblico ministero o al Garante della *privacy* come consentito dall'art. 391-*quater* c.p.p.

Ciò posto, in dottrina sono emerse posizioni divergenti sulla ragionevolezza della differenziazione dell'*iter* per l'acquisizione dei dati di traffico in uscita ed in entrata. Secondo alcuni autori, tale differenziazione procedurale è giustificata dalla maggiore invasività della seconda tipologia di dati[185]. Il traffico telefonico in entrata include infatti informazioni di carattere personale che riguardano non solo l'utente che riceve la chiamata ma anche tutti gli altri soggetti chiamanti (familiari, colleghi di lavoro, dipendenti *etc. etc*.). Ne consegue che l'apprensione di tali dati è suscettibile di ledere non solo la *privacy* del soggetto per cui si procede ma anche quelle di tutti gli altri utenti inevitabilmente coinvolti. Il ricorso ad una procedura rafforzata è volto dunque ad arginare il potenziale *vulnus*[186] che tale operazione comporta.

Il d. lgs. 101/2018 ha aggiunto al terzo comma un'ultima proposizione[187] al fine di armonizzare la disciplina codicistica agli articoli da 12 a 22[188] Regolamento UE 2016/679. Si prevede infatti che i diritti garantiti dalle norme sopracitate del GDPR possano essere esercitati dall'interessato[189] al trattamento dei dati secondo le modalità fissate dall'«articolo 2-*undecies*, comma 3, terzo, quarto e quinto periodo». Sul piano della tecnica normativa, la scelta del legislatore di rinviare addirittura ai periodi contenuti all'interno di un altro articolo del Codice *Privacy* è di ostacolo ad un'agevole comprensione della norma.

---

[185] In senso contrario vedi CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni,* in *Riv. it. dir. e proc. pen*., 2005, 612. L'Autore afferma che «il ragionamento che ha portato il legislatore a distinguere le chiamate in entrata da quelle in uscita, tutelando le prime più delle seconde, rimane piuttosto misterioso».

[186] In tal senso vedi ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, *cit.*, 132.

[187]« …diversamente, i diritti di cui agli *articoli da 12* a *22 del Regolamento* possono essere esercitati con le modalità di cui all'articolo 2-undecies, comma 3, terzo, quarto e quinto periodo».

[188]In breve, gli articoli sopracitati del GDPR riguardano: informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato (art. 12); informazioni da fornire qualora i dati personali siano raccolti presso l'interessato (art. 13); informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato (art. 14); diritto di accesso dell'interessato (art. 15); diritto di rettifica (art. 16); diritto alla cancellazione o diritto all'oblio (art. 17); diritto di limitazione di trattamento (art. 18); obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento (art. 19); diritto alla portabilità dei dati (art. 20); diritto di opposizione (art. 21); processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione (art. 22).

[189] Ai sensi del GDPR con «interessato» si intende «qualsiasi persona fisica a cui si riferiscono i dati che sono oggetto del trattamento». L'interessato può essere solo una persona fisica, e non una persona giuridica, un ente o un'associazione, come chiarito dal considerando 14 del GDPR.

Riguardo al contenuto della previsione basti precisare che l'utente che subisca il trattamento di conservazione dei dati può esercitare nei confronti del gestore tutti i diritti riconosciuti negli articoli citati del GDPR.

La versione attuale dell'articolo 132 prosegue con i commi 4-*ter*, 4-*quater* e 4-*quinquies*, inseriti dall'articolo 10 comma 1, della legge 18 marzo 2008, n. 48 e da quel momento rimasti invariati. Riguardo al loro contenuto e alla c.d. procedura "di congelamento" si rimanda a quanto detto *supra*[190].

Riguardo al comma 5 dell'articolo 132[191], in questa sede basti precisare che il trattamento dei dati effettuato ai sensi del primo comma deve essere effettuato nel rispetto delle prescrizioni del Garante secondo le modalità previste dall'articolo 2-*quinquiedecies*. Tali misure sono previste al fine di garantire l'integrità e la qualità dei dati archiviati[192].

4.5 L'estensione dei tempi di conservazione a sei anni.

Da ultimo, la versione attuale dell'articolo 132 del Codice *Privacy* si contraddistingue per l'inserimento del comma 5-*bis*. Tale interpolazione è di grande rilevanza in quanto opera un totale stravolgimento dei tempi di conservazione fissati dai primi commi della norma in esame. Il grande impatto della previsione di nuovo conio tende a passare inosservata a causa della formulazione poco incisiva operata dal legislatore che si limita a rinviare all'articolo 24 della legge 20 novembre 2017, n. 167 (c.d. legge

[190] Cfr. cap I § 3.4.
[191] Ai sensi dell'art. 132, comma 5 «Il trattamento dei dati per le finalità di cui al comma 1 è effettuato nel rispetto delle misure e degli accorgimenti a garanzia dell'interessato prescritti dal Garante secondo le modalità di cui all'articolo 2-quinquiesdecies, volti a garantire che i dati conservati possiedano i medesimi requisiti di qualità, sicurezza e protezione dei dati in rete, nonché ad indicare le modalità tecniche per la periodica distruzione dei dati, decorsi i termini di cui al comma 1».
[192] Sul punto si tornerà ampiamente nel Cap. III.

europea 2017[193]). È allora necessario procedere ad una lettura sinottica[194] di entrambi gli articoli per cogliere tutte le problematicità del caso.

L'articolo 24[195] dell'atto legislativo sopracitato si pone come un *continuum* rispetto al regime emergenziale previsto dal d.l. 7/2015*[196]* in quanto recepisce le istanze di contrasto alla criminalità organizzata e terroristica e di cooperazione internazionale. Esso prevede che per finalità di accertamento di reati consumati o tentati ricompresi negli articoli 51 comma 3-*quater* c.p.p. e 407 comma 2 lett. a) c.p.p, la conservazione dei dati telefonici e telematici si protrae genericamente per settantadue mesi.

Tale disciplina realizza un dilatamento dei tempi di conservazione indiscriminata per tutte le tipologie di dati di traffico. In deroga alle tempistiche previste al comma 1 e 1-*bis,* la durata di archiviazione del traffico telefonico viene triplicata, passando da due a sei anni mentre quella di traffico telefonico è elevata da uno a sei anni. L'estensione temporale maggiore si riscontra però in merito alle chiamate senza risposta che passano da un termine di appena trenta giorni a settantadue mesi[197].

---

[193] La legge sopracitata recepisce la Direttiva 2017/54/UE approvata il 15 marzo 2017 recante «modifica della direttiva 2003/87/CE al fine di mantenere gli attuali limiti dell'ambito di applicazione relativo alle attività di trasporto aereo e introdurre alcune disposizioni in vista dell'attuazione di una misura mondiale basata sul mercato a partire dal 2021». L'obiettivo primario di tale strumento, non facilmente deducibile dalla sua rubricazione, è quello di far fronte al fenomeno dei *foreign fighters* e del finanziamento del terrorismo. Per far fronte alle straordinarie esigenze di contrasto del terrorismo internazionale emerse negli ultimi anni, l'art. 20 della Direttiva di cui trattasi prevede che «gli Stati membri adottano le misure necessarie affinché le persone, le unità o i servizi incaricati delle indagini o dell'azione penale per i reati (di terrorismo) di cui agli articoli da 3 a 12 dispongono di strumenti di indagine efficaci, quali quelli utilizzati contro la criminalità organizzata o altre forme gravi di criminalità».

[194] L'espressione è di SIGNORATO, *Novità in tema di* data retention, *cit.*, 156.

[195] L'articolo 24 della legge europea 167/2017 è rubricato «Termini di conservazione dei dati di traffico telefonico e telematico». Si ritiene utile riportare il suddetto nella sua interezza: «In attuazione dell'articolo 20 della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio, al fine di garantire strumenti di indagine efficace in considerazione delle straordinarie esigenze di contrasto del terrorismo, anche internazionale, per le finalità dell'accertamento e della repressione dei reati di cui agli articoli 51, comma 3-*quater*, e 407, comma 2, lettera a), del codice di procedura penale il termine di conservazione dei dati di traffico telefonico e telematico nonché dei dati relativi alle chiamate senza risposta, di cui all'articolo 4-bis, commi 1 e 2, del decreto-legge 18 febbraio 2015, n. 7, convertito, con modificazioni, dalla legge 17 aprile 2015, n. 43, è stabilito in settantadue mesi, in deroga a quanto previsto dall'articolo 132, commi 1 e 1-*bis*, del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196».

[196] Per un approfondimento della disciplina richiamata si rimanda al Cap. I § 3.6.

[197] In tal senso BACCARI, *Il trattamento (anche elettronico) dei dati personali per finalità di accertamento dei reati*, in AA. VV., *Cybercrime, cit.*, 1610.

Da una prima lettura della disposizione in esame, sembrerebbe che il legislatore abbia voluto reintrodurre una sorta di "doppio binario"[198] rispetto al reato per cui si procede. Da una parte, laddove l'attività acquisitiva dell'autorità giudiziaria sia finalizzata all'accertamento di reati ordinari si continuerebbero a rispettare le tempistiche di ventiquattro mesi, dodici mesi e trenta giorni previsti dall'articolo 132 Codici *privacy*. Dall'altra, laddove si debba procedere per reati gravi o di matrice terroristica, il periodo di conservazione sarebbe equivalente a settantadue mesi, in base a quanto stabilito dalla legge europea 2017.

Seppur apparentemente lineare, una simile impostazione non tiene in considerazione il fatto che il fornitore, nel momento in cui adempie all'obbligo di archiviazione, non sa né se i dati di traffico verranno acquisiti dall'autorità giudiziaria né per quali tipologie di reato saranno eventualmente richiesti[199]. Ne consegue che il gestore dei servizi è indirettamente obbligato a conservare tutti i dati per un periodo complessivo di sei anni nell'eventualità che questi gli vengano richiesti ai sensi del comma 5-*bis* dell'articolo 132.

In sostanza, a partire dalla novella del 2018, il tempo di archiviazione dei dati deve ritenersi esteso a sei anni in rapporto all'accertamento e alla repressione di tutti i reati[200]. Erodendo l'applicazione dell'art. 132 comma 1 ed 1-*bis*, il regime emergenziale introdotto dalla legge europea del 2017 diventa, di fatto, regime ordinario e oggetto di applicazione generalizzata.

Se, però, la norma del Codice *Privacy* non trova più attuazione in merito ai periodi di conservazione, permane la sua operatività sotto un altro profilo. Le tempistiche previste dai primi due commi dell'articolo 132 determinano non soltanto il periodo di archiviazione dei dati ma anche per quanto tempo sia legittima la loro apprensione da parte dell'autorità giudiziaria. L'articolo 24 della Legge europea si limita ad incidere sul primo aspetto, ma lascia invariato l'*iter* di acquisizione. Ne consegue che la trasmissione agli organi inquirenti e l'acquisizione da parte degli stessi all'interno del

[198] Sulla nozione di "doppio binario" si veda *supra*.
[199] Cfr. SIGNORATO, *Novità in tema di* data retention, *cit.*,160.
[200] Sul punto, BACCARI, *Il trattamento (anche elettronico) dei dati personali per finalità di accertamento dei reati*, 1604. In senso analogo, veda MARCOLINI, *L'istituto della* data retention *dopo la sentenza della corte di giustizia del*, 1590.

procedimento penale continua a rimanere legittima soltanto se si rispettano i limiti previsti dall'articolo 132, comma 3[201].

Da una parte, il fornitore di servizi è chiamato ad archiviare per settantadue mesi tutti i dati, indipendentemente dalla loro tipologia, dall'altra, una volta ricevuta l'istanza di apprensione, è tenuto a verificare il rispetto dei limiti di ventiquattro mesi, dodici mesi e trenta giorni. La trasmissione all'autorità giudiziaria oltre tali previsioni temporali è legittima soltanto qualora si proceda per l'accertamento dei reati di particolare gravità previsti agli articoli 51 comma 3-*quater* c.p.p. e 407 comma 2 lett. a) c.p.p. La tipologia di reato non incide dunque sul periodo di conservazione dei dati di traffico, dal momento che è impossibile conoscere a priori per quale tipo di reato verranno richiesti, ma continua a rilevare per la successiva fase di acquisizione. Come si vedrà meglio in seguito, tale impostazione risulta dissonante rispetto all'approccio europeo in materia, che tende ad affermare la necessità di tempi di archiviazione ristretti a tutela della *privacy*[202].

5. Istituti processuali affini: similitudini ed elementi differenziali (cenni).

La ricognizione dell'assetto normativo, attuale e pregresso, condotta sin qui dimostra che il processo di emancipazione della c.d. *data retention* sia stato definitivamente portato a compimento. È ormai indiscusso che l'istituto *de quo* configuri un mezzo autonomo di ricerca della prova, non assimilabile *in toto* a nessuno degli altri strumenti di indagine[203].

Dal punto di vista dinamico-funzionale, mediante tale strumento si realizza l'immissione all'interno del procedimento penale di *res*, nella specie dei dati di traffico telefonico o telematico, necessarie per l'accertamento dei fatti di reato.

---

[201] Già prima dell'ultima riforma, la giurisprudenza aveva sancito il divieto in capo all'autorità giudiziaria di acquisire successivamente al decorso dei termini previsti dall'art. 132 del d.lgs. 30 giugno 2003 n. 196 i dati di traffico telefonico e telematico, posto il divieto di conservazione degli stessi da parte dei *service provider* oltre il periodo predeterminato. Cfr. Cass. pen., Sez. V. 25 gennaio 2016, n. 7265, nonché Cass. pen., Sez. V, 5 dicembre 2014, n. 156113.

[202] Sul punto si veda quanto affermato dalla CGUE nelle sentenze *Digital Rights Ireland Ltd* e *Tele2 Sverige AB* (Cfr. Cap II).

[203] Cfr. ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, *cit*., 20.

I tentativi di rinvio a categorie giuridiche preesistenti, compiuti in un primo tempo dalla giurisprudenza per colmare il vuoto di disciplina[204], si sono rivelati infatti soluzioni temporanee e soltanto parzialmente soddisfacenti. A partire dai primi interventi del legislatore[205], si è invece assistito ad una graduale emersione degli elementi qualificanti l'attività di acquisizione dei tabulati telefonici tramite l'elaborazione di una disciplina normativa a sé stante. Se da un lato, però, la sua specificità è stata più volte confermata nel processo di stratificazione legislativa, dall'altro non si è mai negata la permanenza di punti di contatto con altri istituti tra di loro eterogenei. Ebbene, l'analisi delle affinità e delle differenze con tali tecniche investigative può essere utile per far emergere la difficoltà di procedere ad *un'actio finium regundorum*[206] della disciplina della c.d. *data retention*.

5.1 Dati "esterni" alla comunicazione e intercettazioni: affinità e differenze.

In primo luogo, è opportuno prendere in considerazione il rapporto intercorrente tra l'istituto *de quo* e l'«intercettazione di conversazioni o comunicazioni telefoniche e di altre forme di comunicazione»[207]. Prima di ricevere apposita disciplina all'interno del Codice *Privacy*, è questo il mezzo di ricerca della prova rispetto al quale si sono compiuti i più frequenti tentativi di assimilazione[208].

La nozione di "intercettazione" è stata oggetto di un orientamento giurisprudenziale[209], ormai consolidato, che ha sopperito all'assenza di definizione espressa all'interno del Codice. In particolare, il Giudice di legittimità ha ricavato dal complesso normativo, che ne prevede l'autorizzazione e ne regola i presupposti, una

---

[204] Cfr. Cap. I § 2.
[205] Cfr. Cap. I §§ 3.1 e 3.2.
[206] Letteralmente tale espressione viene tradotta come "azione di regolamento dei confini". In tale sede siffatto concetto viene utilizzato per esprimere la difficoltà di individuare con precisione l'ambito di applicazione dell'istituto della c.d. *data retention*.
[207] Tale espressione figura nell'art. 266 c.p.p. che fornisce un elenco tassativo di «reati presupposto» per cui è possibile adoperare tale metodologia di indagine. La disciplina delle intercettazioni è collocata all'interno del Titolo III del Libro III del codice di procedura penale interamente dedicato ai «Mezzi di ricerca e di assicurazione della prova».
[208] Si fa riferimento ai tentativi di assimilazione da parte della giurisprudenza nelle sentenze della Corte costituzionale esaminate *supra* Cfr. Cap I § 2.
[209] Basti qui ricordare C. cost., sent. n. 81 del 1993, *cit.*; Cass. Pen. Sez. Un. 23 febbraio 2000, D'Amuri, *cit*.; Cass. pen, Sez. Un., 28 maggio 2003, n. 36747, Torcasio, in *Cass. pen*., 2004, 2094 con nota di FILIPPI, *Le Sezioni Unite decretano la morte dell'agente segreto "attrezzato per il suono"*; commentata anche da FUMU, *Registrazione di colloqui tra presenti effettuata a cura della polizia giudiziaria: insuperabili i limiti alla testimonianza indiretta*, in *Riv. pol*., 2003, p. 762.

caratterizzazione in senso restrittivo del concetto d'intercettazione, in quanto l'unica in sintonia con la disciplina legale di cui al capo IV, titolo III, libro III del c.p.p. Secondo la Corte di cassazione, l'intercettazione "rituale" consiste dunque «nell'apprensione occulta, in tempo reale, del contenuto di una conversazione o di una comunicazione in corso tra due o più persone da parte di altri soggetti, estranei al colloquio»[210].

Accanto alla nozione tradizionale appena delineata, è subentrata la peculiare fattispecie prevista dall'art. 266-*bis*[211], appositamente predisposta dal legislatore per consentire la captazione di flussi di telecomunicazioni. In breve, mediante le «intercettazioni di comunicazioni informatiche o telematiche»[212], le autorità inquirenti sono in grado di apprendere il contenuto di conversazioni su qualsiasi piattaforma informatica questa venga effettuata[213].

Una volta chiarita la nozione di intercettazione, è necessario analizzare i punti di contatto tra l'acquisizione dei dati "esterni" alle comunicazioni e siffatto mezzo di ricerca della prova. È evidente che in entrambi i casi si abbia il coinvolgimento dei medesimi diritti di rango fondamentale. Ambedue gli strumenti istruttori realizzano infatti un'interferenza sia con la riservatezza, sia con la libertà e segretezza delle comunicazioni. Sebbene esista siffatta affinità di natura assiologica, si riscontrano innegabili differenze sul piano tecnico-funzionale che impediscono la piena assimilazione tra i due mezzi di ricerca della prova[214].

Innanzitutto, è necessario sottolineare il diverso oggetto su cui incide l'attività di captazione da parte delle autorità competenti. Laddove gli organi inquirenti dispongano l'acquisizione dei dati di traffico, questi si limitano ad apprendere le informazioni "esterne" inerenti al rapporto comunicativo tra gli utenti. Rimane invece assolutamente preclusa la conoscibilità del contenuto della comunicazione. Al contrario, l'intercettazione delle conversazioni prevede la captazione dell'atto

---

[210] Cfr. par 3 Cass. pen, Sez. Un., 28 maggio 2003, n. 36747, Torcasio, *cit*. In dottrina, v. ILLUMINATI, *La disciplina processuale delle intercettazioni*, Milano, 1983, 27.

[211] L'art. 266-bis c.p.p. è stato introdotto dalla legge 23 dicembre 1993, n. 547 e dispone che « Nei procedimenti relativi ai reati indicati nell'articolo 266, nonché a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche, è consentita l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi».

[212] Così è rubricato l'art. 266-*bis* sopracitato.

[213] Per un approfondimento sul tema delle intercettazioni informatiche si veda DI MARTINO, *Le intercettazioni telematiche e l'ordinamento italiano: una convivenza difficile*, in *Ind. pen*., 2002, 223-224; TESTA, Cybercrime*, intercettazioni telematiche e cooperazione giudiziaria in materia di attacchi ai sistemi informatici*, in *Persona e danno*, *www.personaedanno.it*.

[214] Cfr. DI PAOLO, *La prova informatica*, *cit.*, 741.

comunicativo da parte di un operatore estraneo al colloquio. Emerge con chiarezza, dunque, la maggiore intrusività rispetto al valore della segretezza delle comunicazioni[215].

Anche il momento in cui viene realizzata l'attività di indagine è differente. Da una parte si accede al flusso comunicativo tra due individui nel momento stesso in cui si realizza la conversazione[216]; dall'altra si ha l'acquisizione delle coordinate spaziali e temporali di un rapporto ormai esaurito. Un conto è dunque la captazione contestuale del contenuto comunicativo, un altro accedere al fatto storico della conversazione soltanto a posteriori.

Un terzo punto di divergenza tra i due istituti riguarda il prodotto, in forma di supporto cartaceo o analogico, dell'attività di indagine. Dal momento che l'operazione intercettiva viene realizzata nel corso del procedimento penale da parte degli uffici di polizia che ne dispongono contestuale redazione per iscritto, la prova si ritiene formata in sede processuale[217]. Si tratta a tutti gli effetti di una prova costituenda. Al contrario, la c.d. *data retention*, prevede l'acquisizione dei tabulati telefonici e telematici redatti *ex ante* dai fornitori dei servizi elettronici. Tali documenti hanno origine extra-processuale ed esistono indipendentemente dall'avvio di qualsiasi procedimento penale. Come già affermato *supra*, si è senz'altro in presenza di una prova precostituita.

Altro elemento caratterizzante le intercettazioni è la loro clandestinità. L'attività di ascolto si svolge all'insaputa dei comunicanti grazie a strumenti tecnici che permettono la captazione di conversazioni a distanza[218]. Di contro, l'attività di acquisizione dei tabulati di traffico non può configurarsi come atto "a sorpresa", essendo disposta dall'autorità competente senza l'impiego di particolari accorgimenti che ne precludano la conoscibilità la conoscibilità a terzi. Anzi, la necessaria

---

[215] L'argomento verrà affrontato più ampiamente nel Cap. II.
[216] CAMON, *Le intercettazioni nel processo penale*, *cit.*, 12; BALDUCCI, *Le garanzie nelle intercettazioni tra costituente e legge ordinaria*, Milano, 2002, 30.
[217] Per un approfondimento sulla differenza tra le prove c.d. "precostituite" e "costituende" si veda TONINI, *Manuale di procedura penale*, *cit.*, 249.
[218] Sul punto si veda PARODI, *Le intercettazioni*, Torino, 2002; MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Torino, 2007.

intermediazione dell'ente privato gestore dei servizi depone a favore dell'argomento contrario.

Per tutte le ragioni appena enucleate, risulterebbe eccessivamente forzato il tentativo di ricondurre l'operazione della c.d. *data retention* nel paradigma normativo delle intercettazioni. Si vedrà, però, che le differenze strutturali esistenti tra i due strumenti istruttori tendono ad assottigliarsi nella prassi investigativa, soprattutto grazie ai nuovi strumenti digitali. Risulta, infatti, sempre più difficile distinguere ciò che attiene al "contenuto" della comunicazione da ciò che riguarda informazioni ad essa "esterne"[219].

5.2 Il sequestro probatorio.

Ulteriori elementi di contatto sussistono tra il sequestro penale a fini probatori[220] ai sensi degli articoli 253 c.p.p. [221] e seguenti e la c.d. *data retention*. In entrambi i casi si tratta infatti di metodologie di indagine basate su un'attività di *adprehensio*[222] di *res* preesistenti e formate al di fuori del procedimento penale in corso. Il primo realizza un vincolo di indisponibilità su un bene materiale, mobile o immobile, mediante lo spossessamento coattivo della cosa[223].

Il secondo assicura gli elementi di prova – *rectius*, i tabulati di traffico telefonico – mediante l'acquisizione non nei confronti del titolare della *res,* colui che genera i dati usufruendo del servizio telefonico o telematico, ma nei confronti di chi

---

[219] Sul punto si tornerà ampiamente nel Cap II a cui si rinvia.

[220]Nel nostro ordinamento giuridico, oltre al sequestro probatorio, sono previste altre due tipologie di sequestro ugualmente regolate dal codice di procedura penale. Si tratta del sequestro c.d. "conservativo" e di quello "preventivo" che invece rientrano nel novero delle misure cautelari reali. Il primo, ai sensi dell'art 316 c.p.p, è finalizzato ad assicurare l'esecuzione della sentenza di condanna che potrebbe essere emessa a carico dell'indagato. Il secondo, disciplinato dagli artt. 321-323 c.p.p, viene disposto dal giudice, su richiesta del pubblico ministero, per evitare l'aggravarsi delle conseguenze prodotte dal reato per cui si procede. Per un approfondimento sulle diverse tipologie di sequestro si veda MENDOZA, *Questioni relative alla durata del sequestro ai fini di prova e alla coesistenza tra diversi tipi di sequestro***.** *Nota a Cass. sez. III pen. 1° marzo 1996*, in *Cassazione penale*, 1997, fasc. 3, 823-825.

[221] L'art 253 c.p.p, rubricato «Oggetto e formalità del sequestro» prevede che «L'autorità giudiziaria dispone con decreto motivato il sequestro del corpo del reato e delle cose pertinenti al reato necessarie per l'accertamento dei fatti (comma 1). Sono corpo del reato le cose sulle quali o mediante le quali il reato è stato commesso nonché le cose che ne costituiscono il prodotto, il profitto o il prezzo (comma 2)». La disciplina del sequestro probatorio si inserisce all'interno del Titolo III del Libro III del codice di procedura penale interamente dedicato ai «Mezzi di ricerca e di assicurazione della prova». Per un approfondimento sul punto si veda SCARCELLA, *Presupposti e motivazione del sequestro probatorio*, in *Il libro dell'anno del diritto 2019*, Roma, 2019, 548-560.

[222]Sull'attività di *adprehensio* si rimanda a quanto detto *supra*.

[223] Cfr. TONINI, *Manuale di procedura penale*, *cit.*, 393.

temporaneamente li detiene, in quanto gestore del servizio prescelto. Diversamente dal sequestro, non si appone alcun vincolo di indisponibilità sull'oggetto di apprensione[224], in quanto i fornitori continuano a potere accedere a tali informazioni per lo svolgimento di attività commerciali e di fatturazione.

Prescindendo da tali differenze sul piano attuativo[225], è evidente l'affinità tra i due istituti dal punto di vista funzionale che li rende appartenenti ad un *genus* comune[226]. Al pari del sequestro probatorio[227], l'acquisizione dei tabulati di traffico telefonico e telematico incide su *res* note in via preliminare agli inquirenti e legate da un nesso di pertinenza rispetto al reato per cui si procede. In entrambi i casi, tale relazione di inerenza legittima l'acquisizione degli elementi istruttori da parte dell'autorità giurisdizionale.

5.3 L'ordine di esibizione di atti ai sensi dell'articolo 256 c.p.p.

L'affinità tra i due istituti sopracitati era stata rilevata anzitempo dalla giurisprudenza[228]che aveva assimilato l'acquisizione dei tabulati alla disciplina prevista all'articolo 256 c.p.p.[229] La fattispecie *de qua* dispone una modalità attuativa del sequestro probatorio di natura "consensuale"[230] perché basato sulla collaborazione del detentore del bene oggetto di sequestro[231]. In particolare, è previsto che coloro i

---

[224] Sul punto MELILLO, *L'acquisizione dei tabulati relativi al traffico telefonico fra i limiti normativi ed equivoci giurisprudenziali*, in Cass. Pen., 1999, 477.

[225] Sottolineano le differenze dinamico-funzionali tra il sequestro probatorio e la c.d. *data retention* CALAMANDREI, *Acquisizione dei dati esteriori di una comunicazione*, *cit.*, 1693; CAPRIOLI, *Colloqui riservati e prova penale*, Torino, 2000, 175.

[226]L'espressione è di ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, *cit*., 14.

[227] Sul punto si veda anche BELLANTONI, *Art. 248*, in *Codice di procedura penale commentato*, in GIARDA, SPANGHER (a cura di), Milano, 5° ed., 2017, 2440 e IDEM, *Sequestro probatorio e processo penale*, Piacenza, 2005, 55.

[228] Si veda sul punto la sentenza Corte cost., 11 marzo 1993, n. 81, in *www.cortecostituzionale.it* (v. nota 10) che rinviene nell'articolo 256 c.p.p. l'attuazione per via legislativa della tutela connessa al dovere di riserbo, implicitamente contenuto nell'art. 15 Costituzione. A tale approccio esegetico della Corte costituzionale si erano allineata anche la Cassazione a Sezioni unite. Sul punto si veda Cass., Sez. un., 23 febbraio 2000, D'Amuri, *cit.*, e Cass., Sez. un., 21 giugno, Tammaro, in Cass. Pen., 2001, 400, con nota di MARANDOLA.

[229]L'art 256 c.p.p., rubricato «Dovere di esibizione e di segreti» prevede che « Le persone indicate negli articoli 200 e 201 devono consegnare immediatamente all'autorità giudiziaria, che ne faccia richiesta, gli atti e i documenti, anche in originale se così è ordinato, nonché i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto, e ogni altra cosa esistente presso di esse per ragioni del loro ufficio, incarico, ministero, professione o arte, salvo che dichiarino per iscritto che si tratti di segreto di Stato ovvero di segreto inerente al loro ufficio o professione (comma 1)».

[230]L'espressione è di GIARDA, SPANGHER, GARUTI, BERNASCONI, *Codice di procedura penale commentato*, Assago, 5° ed., 2017.

[231]Cfr. BELLANTONI, *Sequestro probatorio e processo penale*, *cit.*, 55.

quali svolgono un'attività professionale coperta dal segreto d'ufficio o di Stato sono tenuti a fornire i documenti di cui è ordinata l'esibizione da parte dell'autorità giudiziaria.

Tali soggetti, individuati agli articoli 200[232] e 201[233] del codice di procedura penale, sono depositari di una serie di informazioni riguardanti la loro clientela, che non possono divulgare per ragioni deontologiche e correlate al diritto individuale alla segretezza delle comunicazioni[234]. Senza dilungarsi ulteriormente sul contenuto dell'articolo 256 c.p.p., si comprende la ragione per cui l'intermediazione del professionista finalizzata all'ottenimento di documenti personali dei loro clienti sia stata paragonata alla attività di mediazione svolta da parte degli *ISP* per l'apprensione dei tabulati di traffico.

In entrambi i casi, l'attività giurisdizionale fa perno sulla collaborazione di soggetti erogatori di servizi per acquisire dati relativi agli utenti che usufruiscono delle prestazioni prescelte. Eppure, tali analogie non sono sufficienti perché si realizzi un'assimilazione completa tra i due istituti, che rimangono ontologicamente distanti. La *ratio* sottesa alla disciplina prevista dall''articolo 256 c.p.p. nella tutela dell'intrinseca riservatezza che connota alcune attività professionali ed intellettuali. Tale esigenza è invece del tutto estranea all'istituto della c.d. *data retention*, il cui l'interesse primario è la tutela della segretezza delle comunicazioni ai sensi dell'articolo 15 della Costituzione[235].

5.4 Il sequestro di dati informatici presso gli *Internet service provider.*

D'altro canto, l'identità del valore costituzionalmente protetto si rinviene tra l'istituto in esame e la disciplina generale del sequestro di corrispondenza ai sensi

[232] L'articolo 200 del codice di procedura penale a cui si rinvia predispone un elenco tassativo di tutti i soggetti per cui vale la regola del segreto professionale, per ragioni deontologicamente collegate alla loro prestazione lavorativa. Tra gli altri, vi rientrano i medici, i ministri di culto e i giudici.

[233] L'articolo 201 del codice di procedura penale prevede che i «pubblici ufficiali» e i «pubblici impiegati incaricati di un pubblico servizio» sono coperti dal segreto d'ufficio. Sono dunque esentati dal deporre su fatti conosciuti in costanza dell'esercizio di tale funzione pubblica.

[234] Cfr. ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, *cit.*,13.

[235]Inoltre, sottolinea la carenza di idonee salvaguardie difensive predisposte dall'art. 256 c.p.p. FILIPPI, *L'intercettazione di comunicazioni, Milano,* 1997, 28. A causa di tale *deficit* di garanzie, l'Autore si rivela contrario a ricondurre la disciplina dell'acquisizione dei tabulati telefonici a quella predisposta dall'articolo in esame.

dell'articolo. 254 c.p.p[236]. Nonostante tale punto di incidenza, il tentativo di inquadrare l'acquisizione dei tabulati come una *species* del sequestro di corrispondenza si è rivelato fallace fin da tempi risalenti[237].

Ai sensi dell'articolo 254 c.p.p. l'attività di apprensione ha ad oggetto documenti, cartacei o dematerializzati, che attestano una comunicazione scritta non ancora pervenuta al destinatario. L'intervento dell'autorità giudiziaria si colloca infatti mentre la corrispondenza è ancora in transito, situata momentaneamente presso gli uffici postali o il gestore del servizio telematico. Tale interferenza impedisce che la comunicazione già emessa dal mittente pervenga di fatto al destinatario.

Al contrario, ai sensi dell'articolo 132 Codice *Privacy*, l'acquisizione dei tabulati può essere portata a compimento soltanto una volta che il rapporto comunicativo sia stato regolarmente esaurito. Tale approccio "neutrale" rispetto all'attività comunicativa, non presente nell'art. 254 c.p.p, ricorre nella disciplina prevista dall'articolo 254-*bis*[238].

Siffatta norma è stata introdotta dalla legge 48/2008[239] e prevede una disciplina specifica sul «sequestro dei dati informatici presso i gestori di servizi informatici, telematici e telefonici». L'intento che ha mosso il legislatore è stato quello di assicurare l'integrità delle informazioni[240] oggetto di sequestro senza pregiudicare il corretto funzionamento dei servizi informatici gestito da parte degli *Internet Service Providers*[241].

---

[236] L'art. 254, comma 1, c.p.p. dispone che « Presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni è consentito procedere al sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica, che l'autorità giudiziaria abbia fondato motivo di ritenere spediti dall'imputato o a lui diretti, anche sotto nome diverso o per mezzo di persona diversa, o che comunque possono avere relazione con il reato».

[237] Si sono espressi contrariamente all'assimilazione tra la c.d. *data retention* e il sequestro di corrispondenza CALAMANDREI, *Acquisizione dei dati esteriori di una comunicazione*, *cit.*, 1693 e MELILLO, *L'acquisizione dei tabulati relativi al traffico telefonico fra i limiti normativi ed equivoci giurisprudenziali*, *cit.*, 477.

[238] Per completezza espositiva, si ritiene utile riportare per intero l'art. 254-*bis* che dispone che «L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro non modificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali».

[239] Cfr. Cap I § 3.4.

[240] Sul problema dell'integrità della *digital evidence* si rimanda al Cap. III.

[241] Per una definizione di Internet Service Providers si rimanda a Cap. I § 4.2.

L'articolo in esame consente all'autorità giudiziaria procedente di acquisire i dati informatici *ab origine*[242]– *rectius*, i c.d. *files di log* [243]– «mediante copia di essi su adeguato supporto»[244]. Con l'ultima espressione, si fa riferimento alla procedura di clonazione del contenuto dell'*hard-disk* del *server*[245] presso l'*ISP* e al suo trasferimento su una memoria esterna. Grazie a questa metodologia, ormai cristallizzata in una serie di protocolli in ambito scientifico, si garantisce la possibilità di analizzare più volte lo stesso supporto senza il rischio di alterazione del suo contenuto, consentendo la ripetibilità dell'attività di acquisizione probatoria[246]. Si rende possibile anche l'analisi di eventuali parti vuote dell'*hard-disk* che possono contenere *file* cancellati non altrimenti rilevabili con la scansione ordinaria[247].

La procedura operativa può avere ad oggetto soltanto dati «di traffico e di ubicazione»[248] con l'esclusione di tutte le informazioni digitali che non ricadono nella predetta categoria. Secondo la suddetta previsione, verrebbe a crearsi una sovrapposizione normativa *ratione materiae* tra l'articolo 254-*bis* e la disciplina del *data retention* prevista dall'articolo 132 del Codice *privacy*. L'oggetto delle due disposizioni è infatti apparentemente identico: in entrambi i casi è prevista una

---

[242]In dottrina, sulla nozione di dati informatici v. DI PAOLO, *La prova informatica*, *cit.*, 737. L'Autore li definisce «informazioni espresse in codice binario — ossia in sequenze di numeri, zero e uno, i cosiddetti *bit* — contenute nelle memorie di *computer* o altri dispositivi informatici, oppure circolanti nella rete». In senso analogo, si veda RUSSO, SCIUTO, *Habeas data e informatica*, Milano, 2011, 34.

[243]Con l'espressione "log" si fa riferimento alla registrazione sequenziale e cronologica delle operazioni effettuate all'interno di un sistema informatico. Siffatte attività possono essere effettuate da un utente oppure avvenire in modo totalmente automatizzato. Le procedure di *logging* consistono dunque nella memorizzazione di tali attività che danno luogo ad una serie di registrazioni denominate, per l'appunto, "files di log". Sul punto si veda PICOTTI, *Diritto penale e tecnologie informatiche*, *cit.*, 61.

[244] Siffatta modalità acquisitiva viene efficacemente descritta da ATERNO, *Le investigazioni informatiche e l'acquisizione della prova digitale*, in *Giur. merito,* 2013, 955. Tra i vari contributi in materia v. anche LUPÁRIA, *La ratifica della Convenzione Cyber Crime del Consiglio d'Europa*, *cit*. 730; LORENZETTO, *Utilizzabilità dei dati informatici incorporati su* computer *in sequestro: dal contenitore al contenuto passando per la copia*, in *Cass. pen.*, 2010, 532; IDEM, Le attività urgenti di investigazione informatica e telematica, in LUPÀRIA (a cura di), Sistema penale e criminalità informatica, Milano, 2009, 152

[245] L'*hard disk* o disco rigido è uno strumento utilizzato per la memorizzazione a lungo termine dei dati di un *computer*. La capacità è, in genere, espressa in *gigabyte* (GB). In pratica, si tratta di una memoria magnetica, realizzata in ferro, in cui vengono inscritti i dati raccolti magnetizzando o smagnetizzando la sua superficie. Sul punto si veda DI PAOLO, *La prova informatica*, in *Enc. Dir.*, 2013, 737.

[246] SIGNORATO, *Novità in tema di* data retention, *cit.*, 18.

[247] Sottolineano la ripetibilità dell'atto di acquisizione probatoria ai sensi dell'art. 254-*bis* c.p.p. CERQUA*, Ancora dubbi e incertezze sull'acquisizione della corrispondenza elettronica, in Dir. Pen. Cont. 23 luglio 2015;* LORENZETTO, *Utilizzabilità dei dati informatici incorporati su* computer *in sequestro: dal contenitore al contenuto passando per la copia*, in *Cass. pen.*, 2010, 534.

[248]Cfr. art. 254-*bis* c.p.p.

modalità di acquisizione dei dati detenuti da fornitori di servizi informatici in capo ai quali è previsto l'obbligo di conservazione.

L'unica differenza tra i due istituti sembrerebbe rinvenirsi nel fatto che non sono inclusi nell'ambito di applicazione dell'articolo 254-*bis* i tabulati di traffico telefonico, i quali potrebbero essere acquisiti soltanto mediante la procedura prevista nel Codice *Privacy*. Riguardo a tutti gli altri dati, verrebbe invece riconosciuto in capo al pubblico ministero un potere di fatto illimitato perché non sottoposto a tutte le restrizioni temporali previste all'articolo 132.

Una simile lettura sinottica delle norme *de quibus* andrebbe a circoscrivere eccessivamente il raggio di applicazione della disposizione del Codice *Privacy*. Al fine di superare tali criticità, la dottrina e la giurisprudenza concordano su una interpretazione della norma che tenga in considerazione ragioni di carattere sistematico. Secondo tale approccio, l'articolo 254-*bis* rappresenterebbe un corollario necessario dell'articolo 254 del codice di procedura penale con cui va letto in combinato disposto[249].

La topografia della norma all'interno del codice di procedura penale costituisce infatti elemento rilevatore dell'intento del legislatore, il quale, lungi dal voler costituire una figura autonoma di sequestro, ne disciplina un suo *modus operandi*. La procedura *de quo* ha ad oggetto soltanto dati digitali e può essere usufruita dall'autorità giudiziaria limitatamente ai casi previsti dell'articolo 254 c.p.p., comma 1.

Viene ritagliato dunque un autonomo spazio applicativo del sequestro avente ad oggetto dati informatici costituenti corpo del reato o cose pertinenti allo stesso che può essere realizzato attraverso la procedura prevista dall'art. 254-*bis*. Tale modalità, finalizzata a garantire l'integrità dei dati digitali, è facoltativa e non obbligatoria rispetto all'alternativa apprensione del supporto materiale in cui questi sono conservati[250].

---

[249] Ciò si evince dalla clausola di apertura della norma che richiama esplicitamente la disciplina del sequestro previamente enucleata. L'espressione in esame andrebbe a richiamare non solo le modalità con cui procede l'autorità giurisdizionale ma anche tutti i casi in cui tale mezzo di ricerca della prova sia consentito. In tal senso si veda CISTERNA, *Il legislatore interviene ancora sulla data retention, ma non è ancora finita*, in *Dir. pen e proc*. 2009, 320.

[250] Sul punto si veda anche DI PAOLO, *La prova informatica*, *cit.*, 755 secondo cui «l'art. 254-*bis* disciplinerebbe il *quomodo*, ma non l'*an* del decreto di sequestro, il quale resterebbe quindi consentito soltanto nei casi previsti dal comma 1 dell'art. 254».

Ne consegue che, davanti all'esigenza di apprensione di dati informatici, l'autorità competente si trova davanti ad una triplice possibilità: da un lato può acquisire l'*hard-disk* presso il *server* dell'*ISP*[251], secondo la modalità ordinaria prevista all'articolo 254 c.p.p., dall'altro può effettuare la copiatura dei dati, con tutti i vantaggi che essa comporta, ai sensi dell'art. 254-*bis*. Come terza ipotesi, qualora l'attività di indagine abbia ad oggetto i dati originali di traffico, si può procedere alla loro acquisizione secondo l'*iter* previsto dall'articolo 132 del Codice *Privacy*.

In ogni caso, qualsiasi sia la modalità prescelta, tali dati verranno conservati e adeguatamente protetti secondo le tempistiche previste dal Codice *Privacy*. Anche quando le esigenze probatorie legate all'accertamento penale vengano soddisfatte mediante l'acquisizione in copia ai sensi dell'articolo 254-*bis*, ciò dovrà quindi avvenire nel rispetto dei limiti temporali previsti dall'articolo 132.

In conclusione, secondo l'interpretazione sistematica più diffusa in dottrina, non si avrebbe alcuna sovrapposizione normativa tra l'articolo 254-*bis* c.p.p. e la disciplina contenuta nel Codice *Privacy.* Siffatta impostazione, mediante la quale si riconosce agli istituti un'autonomia applicativa, elimina soltanto in parte le interferenze esistenti tra i due mezzi di ricerca della prova. Ciò a riprova di quanto sia oltremodo difficile segnare un "confine" preciso tra la disciplina della c.d. *data retention* e le altre attività istruttorie, soprattutto in "ambiente digitale"[252].

5.5 I nuovi strumenti della tecnica.

Dopo aver esaminato i potenziali punti di incidenza tra la disciplina dell'articolo 132 Codice *Privacy* e i mezzi di ricerca della prova tipizzati nel Codice di procedura penale, è utile procedere all'analisi di alcuni strumenti ad alto contenuto tecnologico[253], ancora privi di una normativa *ad hoc*. Affermatesi con forza nella prassi[254], questi sono spesso essenziali per una efficiente conduzione dell'attività di indagine e presentano affinità assai evidenti con il c.d. *data retention.*

---

[251] Sulla definizione di *Internet Service Provider* si veda *supra*.

[252] L'espressione è DI PAOLO, *La prova informatica*, *cit.*, 761

[253] Sul proliferarsi di nuove tecnologie investigative non ancora tipizzate all'interno del codice di procedura penale si veda *Intro.*

[254]Sul punto si veda SCALFATI, *Le indagini atipiche*, Torino, 2014, XV. L'Autore si riferisce all'insieme delle operazioni investigative emerse nella pratica della polizia giudiziaria con l'espressione "indagini a tipiche". Si tratta di una categoria aperta e con i contorni sfumati soprattutto a causa della mancata codificazione da parte del legislatore.

Innanzitutto, vengono in rilievo forme di sorveglianza a distanza e operazioni di controllo telefonico che incidono con intensità variabile sul principio della segretezza di comunicazioni ai sensi dell'articolo 15 Cost[255].

Tra di esse si annovera il c.d. *DigeSystem,* utilizzato dalle forze di polizia italiana negli anni '90. Mediante tale apparato si effettuava il monitoraggio su apparecchi telefonici pubblici situati in una stessa macro-area interessata da significativi eventi criminali. In alternativa alle intercettazioni analogiche[256] che richiedevano l'impiego di un'ingente quantità di risorse, ogni apparato riusciva a tenere sotto controllo fino a 32 utenze, di cui era in grado di rilevare le chiamate in uscita verso utenze private. Gli inquirenti potevano disporre anche di filtri modulabili a seconda delle esigenze del caso specifico per selezionare utenze con un determinato prefisso, afferenti a province preselezionate.

Non producendo alcuna interferenza rispetto alle comunicazioni effettuate dall'utenza posta sotto controllo, tale tecnica non rientra nella nozione di intercettazione. Secondo la giurisprudenza di legittimità[257], rientravano infatti nel paradigma dell'acquisizione dei tabulati telefonici sia sul piano del livello di incidenza nella sfera della riservatezza, sia su quello delle garanzie processuali[258].

In epoca risalente, veniva utilizzato frequentemente a scopo investigativo anche il c.d. blocco telefonico[259] tramite il quale venivano identificati il mittente, il destinatario, i tempi e la durata della conversazione telefonica. A differenza dell'istituto precedente, l'autorità inquirente non si limitava ad apprendere i dati esterni associati alla conversazione telefonica ma era in grado di captarne in contenuto, senza interrompere la comunicazione. Tale tecnica realizzava dunque una rimarchevole

---

[255] Vedi SIGNORATO, *Novità in tema di* data retention*, cit.*, 20.

[256]Per la distinzione tra metodo analogico (basato sulla rappresentazione mediante grandezze fisiche variabili in proporzione rispetto al fenomeno da riprodurre) e metodo digitale (basato sulla rappresentazione mediante grandezze fisiche variabili a intervalli regolari nel tempo), v. TONINI, *Documento informatico e giusto processo*, in *Dir. pen. proc.*, 2009, 403-404. A seconda del mezzo tecnico utilizzato per captare in tempo reale le comunicazioni vocali si parla di intercettazioni "analogiche" (realizzate mediante trascrizione o videoregistrazione) o "digitali" (incise su disco rigido, *cd*, chiavetta *usb*).

[257] Cfr. Cass. Pen. Sez. IV, 23 giugno 2009, n. 38160, L.R.A, in *CED* n. 244384; Cass., Pen. Sez. II, 25 ottobre 2005, Piscopo, in *Giust. Pen*., 2006, 707.

[258] Per l'utilizzo dei dati provenienti dalle utenze pubbliche sottoposte al *DigeSystem* si riteneva sufficiente la semplice autorizzazione del P.M. Sul punto ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, *cit.*, nota 54.

[259] Si veda FILIPPI, *Il rilevamento del «tracciato axe»: una nuova denominazione per una vecchia tecnica d'indagine*, *Giur. It.*, 1999. 8-9.

ingerenza sulla segretezza delle comunicazioni in quanto effettuava una vera e propria intercettazione fonica.

Il perfezionamento tecnologico di tale tecnica ha dato luogo al c.d. rilevamento del "tracciato AXE", così denominato in base al nome dello strumento tuttora utilizzato dagli operatori. Tale metodologia investigativa consente di identificare il numero e la provenienza del chiamante, mediante controlli effettuati sugli impianti telefonici. Rientra nel novero del c.d. «tracciamento delle comunicazioni[260]» mediante il quale si realizza un monitoraggio in tempo reale degli spostamenti dell'utenza telefonica mobile.

La geolocalizzazione del telefono, e in via mediata del suo utente, può realizzarsi in due modi: attraverso il tracciamento della comunicazione nel momento in cui questa è effettuata (tramite la identificazione della cella telefonica) oppure mediante la localizzazione dell'utenza telefonica, indipendentemente dal fatto che abbia realizzato o meno un atto comunicativo. Questa seconda modalità viene utilizzata in via residuale quando le autorità inquirenti sono in possesso del solo numero seriale associato all'apparecchio telefonico che si vuole tracciare[261].

Nel caso di specie, il controllo del dispositivo non viene effettuato tramite il monitoraggio delle chiamate effettuate dal suo proprietario e i dati che si acquisiscono non sono correlati al traffico telefonico. Tale operazione, seppur non espressamente regolata dal legislatore, può trovare riconoscimento[262] negli artt. 126 e 127[263] del Codice *privacy* in cui è contemplato il trattamento dei «dati relativi all'ubicazione[264] diversi dai dati relativi al traffico». Qualora si disponga il monitoraggio delle chiamate, i dati di ubicazione ottenuti tramite il tracciamento del dispositivo sono inquadrabili a tutti gli effetti come "dati esterni" alla comunicazione. La distinzione tra le due

---

[260] Tale terminologia ricorre soltanto all'articolo 226, comma 4, delle disposizioni di attuazione al c.p.p. in cui si parla di «tracciamento delle comunicazioni» nel limitato ambito delle investigazioni preventive.

[261] Si fa qui riferimento al c.d. Codice IMEI (in acronimo dall'inglese *International Mobile Equipe Identity*, ovvero Identità Internazionale dei terminali mobili). Si tratta di un codice di 15 cifre diviso in quattro sezioni unico per ogni dispositivo.

[262] In tal senso FILIPPI, *Intercettazione*, in FERRUA, MARZADURI, SPANGHER (a cura di), *La prova penale*, Torino, 2013, 926 ss.

[263] Per approfondire si veda BENE, *Il pedinamento elettronico: truismi e problemi spinosi*, in AA.VV., *Le indagini atipiche,* a cura di SCALFATI, Torino, 2014, 347.

[264] Ai sensi dell'art. 4, comma 2 lett i) del codice *Privacy*, con «dati relativi all'ubicazione» si intende «ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica, che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico».

modalità di attuazione del c.d. "tracciamento AXE" non è priva di riflessi sulla questione relativa alle analogie esistenti con la c.d. *data retention*.

Sulla base di quanto detto sopra, infatti, la localizzazione di un soggetto può effettuarsi attraverso la semplice acquisizione dei tabulati di traffico che si riferiscono ad utenze "mobili". Gli stessi, oltre a documentare il dato storico della comunicazione e dei relativi tempi di durata, sono in grado di individuare anche il luogo in cui il soggetto di trova al momento della chiamata, mediante l'identificazione della "torre-radio" cui è stata agganciata l'utenza. In tal modo dal tabulato è possibile ricavare il "tracciamento" degli spostamenti dell'utenza telefonica, e in via mediata del suo detentore[265]. Operazione consentita dal fatto che quando un apparecchio telefonico si sposta nel territorio da una cella, *rectius*, torre-radio, ad un'altra deve rinegoziare la connessione con la rete telefonica e, quindi, diventa ricostruibile il movimento anche in assenza di chiamata[266].

5.6 L'estrazione di dati dal *display* del dispositivo telefonico altrui.

Osservazioni in parte analoghe si possono fare relativamente alla lettura e alla successiva operazione di acquisizione da parte delle autorità inquirenti di dati impressi nel *display*[267] e nella memoria[268] del telefono cellulare[269]. Si tratta di una prassi investigativa secondo cui, una volta rinvenuto e repertato l'apparecchio di telefonia sulla scena del crimine, la polizia procede all'apprensione informale delle informazioni personali contenute al suo interno.

Pur non trovando riscontro nel codice di procedura penale, tale operazione è stata avallata dalla giurisprudenza di legittimità[270], secondo cui l'apprensione dei dati

---

[265] Sul punto si veda DI PAOLO, *Tecnologie del controllo e prova penale: l'esperienza statunitense e spunti per la comparazione*, Padova 2008, 262.

[266] Tale sistema è noto come "*cell site analysis"* e permette di geolocalizzare il dispositivo mobile qualunque attività su di esso sia rilevata. Sono incluse non solo la ricezione o l'effettuazione di chiamate ma anche messaggistica istantanea o connessione ad *Internet*. Sul punto si veda DINACCI, Localizzazione attraverso celle telefoniche, in AA. VV., *Le indagini atipiche,* SCALFATI (a cura di), Torino, 2014, 370.

[267] Con il termine "display" (ad esempio di un computer o di un telefono) si fa riferimento allo schermo di visualizzazione dei dati in forma grafica o numerica. Cfr. SCACCIANOCE, *Approvvigionamento di flussi e dati tramite il dispositivo telefonico altrui, cit.*, 30.

[268] Tutti i dati reperibili in un dispositivo possono trovarsi nella carta SIM (o *Subscriber Identity Mobile*), sulla memoria rimovibile, o ancora sulla memoria interna, collocata nel *software* del telefono. Sul punto SCACCIANOCE, *Approvvigionamento di flussi e dati tramite il dispositivo telefonico altrui, cit.*, 30.

[269] Sulla definizione di telefono cellulare o utenza mobile si rimanda a quanto detto *supra*.

[270] Cfr. Cass. Pen., Sez. IV, 8 maggio 2003, Lanzetta, in *Cass. Pen*., 2006, 536, con nota di RENZETTI; nello stesso senso, Cass. Pen., Sez. I, 13 marzo 2013, Romeo, in *Giust. Pen*., 2013, III, 56.

contenuti nell'apparecchio telefonico rientrerebbe «tra gli atti urgenti demandati agli organi della polizia giudiziaria ai sensi degli artt. 55 e 348 c.p.p.[271]». Secondo tale assunto gli organi inquirenti potrebbero procedere ad una ricognizione dei dati e, in un secondo momento, ad una loro acquisizione senza richiedere alcuna autorizzazione all'autorità giudiziaria. Tale approccio della giurisprudenza non è condivisibile in quanto legittima una operazione lesiva della segretezza delle comunicazioni senza imporre, in cambio, alcuna garanzia processuale[272].

Ai fini di una corretta individuazione del regime applicabile a tale operazione, è necessario tenere conto innanzitutto dell'eterogeneità di informazioni contenute sul *display* e nella memoria di un cellulare. In tale ampia categoria rientrano sia i flussi comunicativi sotto forma di messaggi telefonici (*SMS o MMS*), *e-mail* e *chat* di messaggistica istantanea sia i dati esteriori ai contenuti comunicativi (traffico chiamate, giorno ora e durata della conversazione).

Ai fini della presente indagine, è necessario focalizzarsi soltanto sull'ultima tipologia di dati, in quanto analoghi dal punto di vista contenutistico a quelli riconducibili ai tabulati di traffico telefonico e telematico. Molteplici sono infatti le affinità tra tale prassi operativa e l'istituto della *data retention,* in quanto in entrambi i casi l'attività apprensiva ha ad oggetto dati esteriori di comunicazioni che risultano utili per l'accertamento di fatti storici di reato. Nel caso in esame, però, l'autorità giudiziaria non necessita della intermediazione dell'ente gestore dei servizi digitali per entrare in possesso di tali informazioni.

---

[271] Il combinato disposto degli. artt. 55 c.p.p. recante «Funzioni della polizia giudiziaria» e 348 c.p.p. rubricato «Assicurazione delle fonti di prova» dispone il potere autonomo della p.g. nello svolgimento di attività di acquisizione e assicurazione delle fonti di prova. Secondo la giurisprudenza prevalente, dalle norme *de quibus* emerge «il principio dell'atipicità degli atti ai indagine della polizia giudiziaria», la quale, ha il «potere-dovere di compiere di propria iniziativa, finchè non abbia ricevuto dal pubblico ministero direttive di carattere generale o deleghe per singole attività investigative, tutte le indagini che ritiene necessarie ai fini dell'accertamento del reato».

[272]Sul punto, si veda LORENZETTO, *Le attività urgenti di investigazione informatica e telematica*, in LUPÀRIA (a cura di), *Sistema penale e criminalità informatica*, Milano, 2009, 135. L'Autrice sottolinea che le indifferibili operazioni informatiche ad iniziativa della p.g. non possono mai prescindere da un provvedimento motivato del pubblico ministero. In senso analogo v. RENZETTI, *Acquisizione dei dati segnalati sul* display *del cellulare: il rischio di una violazione dell'art. 15 Cost.*, in *Cass. Pen.* 2006, 542.

Una volta rinvenuto l'apparecchio telefonico nel *locus commissi delicti*[273], può avere accesso immediato[274] a tutto il suo contenuto immediatamente, senza attendere la fattiva collaborazione del terzo fornitore. A causa di tale differenza sostanziale e procedurale non è possibile far rientrare tale prassi operativa nell'ambito di applicazione dell'articolo 132 del Codice *privacy.* Altrettanto vano è il tentativo di ricondurre l'attività *de qua* alla disciplina delle intercettazioni, dal momento che questa non realizza una captazione del contenuto delle comunicazioni.

Tramite questa breve rappresentazione delle prassi operative affini alla c.d. *data retention*, emerge una situazione di incertezza generale nell'applicare ad esse le tradizionali categorie concettuali contenute nel Codice. In effetti, soprattutto in merito a alcuni profili, risulta difficile utilizzare criteri ermeneutici "pre-tecnologici"[275]. È, dunque, auspicabile un ripensamento da parte del legislatore dell'intera materia a partire dall'inquadramento dei diritti fondamentali coinvolti da tali attività investigative. Una volta chiariti quali siano i valori di rango costituzionale compromessi, sarà più facile porre le basi per un sistema processuale idoneo ad affrontare le sfide del progresso tecnologico.

Questo sarà, dunque, il metodo di ricerca che si seguirà nei prossimi capitoli.

---

[273] Si fa qui riferimento alla nozione tradizionale di "locus commissi delicti", e cioè al luogo in cui si è realizzata la condotta criminosa, in tutto o in parte, ovvero ove si sia verificato l'evento. Sul punto si veda MARINUCCI, DOLCINI, GATTA, *Manuale di diritto penale. Parte generale*, Milano, 2018, 146.

[274] Ciò posto, è sbagliato dedurre che l'operazione atipica in esame sia completamente priva di disciplina e possa dunque essere svolta liberamente dalle autorità inquirenti. La polizia giudiziaria che venga in contatto con il reperto digitale dovrà infatti conformarsi alla procedura del sequestro prevista per gli atti di indagine urgenti ai sensi dell'articolo 354 comma 2 c.p.p. In primo luogo, sarà tenuta a cristallizzare la "*scena criminis* digitale" per assicurare l'integrità dei dati in essa contenuti, in secondo luogo potrà procedere al sequestro del telefono cellulare e all'estrapolazione dei suoi contenuti ai sensi dell'articolo 355 c.p.p. L'art 355 c.p.p. rubricato «Convalida del sequestro e suo riesame» prevede che la polizia giudiziaria che abbia provveduto al sequestro enuncia nel relativo verbale il motivo del provvedimento e ne attende la convalida entro 48 ore successive da parte del P.M. In tal senso, si veda BELLANTONI, *Sequestro probatorio e processo penale*, *cit.*, 349. Secondo l'Autore, il sequestro si impone come «alternativa obbligata» laddove si predispongano operazioni assicurative delle tracce digitali perché in mancanza di idonee garanzie processuali si potrebbe cagionare la irreversibile alterazione o distruzione del reperto digitale. Analogamente, LUPÀRIA, *La ratifica della Convenzione* Cybercrime *del consiglio d'Europa*, *cit.*, 721; TONINI, *Documento informatico e giusto processo*, *cit.*, 406.

[275] L'espressione è di DI PAOLO, *La prova informatica*, *cit.*, 761.

CAPITOLO II

I DIRITTI FONDAMENTALI COINVOLTI DALLA DISCIPLINA DELLA CONSERVAZIONE DEI DATI DI TRAFFICO: TRA PARADIGMI COSTITUZIONALI E CARTE EUROPEE DEI DIRITTI

1. Note introduttive.

Nel capitolo precedente, in cui si è cercato di fornire le coordinate normative essenziali dell'istituto della c.d. *data retention*, è emerso che la conservazione e l'accesso da parte delle pubbliche autorità ai dati di traffico interferiscono inevitabilmente con la tutela dei diritti fondamentali. Rientrano nella cornice di valori coinvolti, a titolo meramente esemplificativo: il diritto alla segretezza sul fatto storico della comunicazione, la tutela della riservatezza e la libera determinazione dei propri dati personali[276]. Tutte situazioni giuridiche soggettive inviolabili della persona[277].

Gli stessi sono stati – e tuttora sono – sottoposti a costanti pressioni e limitazioni nel tortuoso percorso di individuazione di un corretto bilanciamento con le esigenze di sicurezza nell'ambito della prevenzione e della lotta al terrorismo[278]. Se l'utilità dell'acquisizione dei flussi informativi ai fini di indagine è ormai indubbia[279], in tale sede è necessario approfondire quali e in che modo siano lesi, di fatto, i diritti dell'individuo sopra richiamati. Soltanto a seguito di un'approfondita disamina di natura costituzionale e sovranazionale, si sarà, infatti, in grado di capire se il tanto "agognato" equilibrio tra interessi contrapposti che incidono sulla conservazione dei dati sia stato raggiunto.

---

[276] Sul punto, v. CONTI, *Sicurezza e riservatezza*, in Dir. pen. e proc., 2019, 11, 1572; in conformità v. D'AGOSTINO, *La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al D.Lgs. 10 agosto 2018, n. 101, in Archivio penale*, 2019, 1; PATRONO, Privacy *e vita privata*, in Enc. dir., vol. XXXV, Milano, 1986, 574.

[277] È, infatti, ormai consolidato l'orientamento secondo cui la libertà e la segretezza della corrispondenza e, in senso lato delle comunicazioni, rientri insieme alla libertà di domicilio, nei diritti inviolabili della persona tutelati dall'art. 2 Cost. Sul punto, si veda in dottrina, per tutti, BARILE, CHELI, *Corrispondenza (libertà di)*, in *Enc. Dir*., vol. X, Milano, 1962, 744.

[278] Così CAGGIANO, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione,* in *Medialaws – Rivista dir. media*, 2018, fasc. 2, 64.

[279] Cfr. Cap I.

A tal fine, verranno presi in considerazione tutti i diritti di libertà che entrano in contrasto con l'attuale normativa della *data retention,* cristallizzata nel Codice *Privacy*. Nel contesto degli strumenti di indagine di "nuova generazione"[280], le esigenze di tutela di siffatti valori si sono ampliate, in corrispondenza dell'accresciuta possibilità di acquisire e condividere le suddette informazioni. Alla crescente esposizione pubblica "sfera privata"[281] dell'individuo, corrisponde un innalzamento del grado di attenzione verso la salvaguardia dei diritti fondamentali, soprattutto in rapporto alla *privacy*. Essa diventa oggetto di garanzia "multivello" (c.d. *multilevel protection*) all'interno di un sistema "reticolare" in cui concorrono alla sua tutela più ordinamenti giuridici tra loro correlati[282].

Sotto questo profilo, vengono in rilievo, oltre allo statuto costituzionale, la Convenzione europea dei diritti dell'uomo e delle libertà fondamentali e la Carta dei diritti fondamentali dell'Unione europea, così come interpretata dalla giurisprudenza della Corte di Lussemburgo.

Con l'obiettivo delineare uno scenario il più possibile organico dei diritti fondamentali coinvolti dalla c.d. *data retention,* seguirà un'analisi dell'assiologia costituzionale e delle fonti sovranazionali sopra citate. In conclusione, si passerà allo studio degli approdi giurisprudenziali che hanno analizzato le interferenze esistenti tra l'utilizzo di tali informazioni a fini investigativi e la tutela "sfera privata" dell'individuo.

2. Il diritto alla segretezza delle comunicazioni.

Fin da tempi risalenti, si è rilevato, che l'attività di conservazione dei dati produce un'interferenza particolarmente vistosa con la libertà e alla segretezza delle comunicazioni, prevista all'articolo 15 della Costituzione[283]. Siffatta norma riconosce

---

[280] L'espressione è di ANDOLINA, *L'ammissibilità degli strumenti di captazione dei dati personali tra standard di tutela della* privacy *e onde eversive*, in *Arch. pen.*, 2015, n. 3, 916.

[281] Sul punto v. sent. Corte cost., n. 366 del 1991, in Giur. cost, 1991, 2914, in cui la c.d. "sfera privata" è definita lo «spazio vitale che circonda la persona». In dottrina, sulla sfera di riserbo essenziale al pieno sviluppo della persona umana v. PISANI, *La tutela penale della "riservatezza": aspetti processuali*, in *Riv. it. dir. proc. pen*., 1967, 785).

[282] Sul punto, v. ANDOLINA, *L'ammissibilità degli strumenti di captazione dei dati personali tra standard di tutela della* privacy *e onde eversive*, cit., 918.

[283] L'articolo 15 Cost. prevede che:
«La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili (comma 1).

in capo al mittente e al destinatario[284] il diritto che la comunicazione effettuata resti "libera e segreta" e non conoscibile a terzi. La disposizione in esame prevede, dunque, la tutela congiunta di due situazioni giuridiche soggettive distinte ma complementari[285]. La prima assicura all'individuo la libertà in senso stretto di poter comunicare e corrispondere con altre persone, senza che la conversazione subisca interruzioni o interferenze. La seconda, invece, riconosce al singolo la pretesa di impedire la conoscibilità del contenuto dell'atto comunicativo a soggetti diversi dai destinatari individuati dal mittente[286].

La scomposizione del diritto fondamentale in due momenti distinti, dunque, garantisce, *in primis,* una tutela specifica del "momento dinamico"[287] della comunicazione, durante il quale si instaura il rapporto tra più soggetti determinati, garantendo all'individuo la libertà di comunicare con qualunque modalità si prescelga. *In secundis*, assicura la tutela del "momento statico" durante il quale, una volta che la conversazione sia terminata, si preclude che terzi vengano a conoscenza del suo contenuto[288]. Quest'ultimo aspetto rappresenta un corollario necessario del primo, poiché, in linea di principio, la corrispondenza, e più in generale gli strumenti di comunicazione, in tanto possono dirsi liberi in quanto ne sia assicurata la segretezza[289].

La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge (comma 2).».

[284] La disposizione in esame non specifica infatti il titolare del diritto inviolabile. Pertanto, deve essere assicurata pari dignità ed eguale tutela sia a chi effettua la comunicazione sia a chi la riceva. Proprio in merito al rapporto tra autore e destinatario della comunicazione, e da sottolineare la differenza tra l'art. 15 e l'art. 21 Cost. In quest'ultimo articolo, la tutela della libertà di manifestazione del pensiero non implica anche la tutela della sua segretezza perché non è preso in considerazione un destinatario determinato ma una pluralità di soggetti raggiunti da mezzi di comunicazione di massa. Cfr. CLEMENTI, *La Costituzione italiana: commento articolo per articolo*, Bologna, 2018, 53.

[285] Così CARUSO, *La libertà e la segretezza delle comunicazioni nell'ordinamento nazionale, in Forum di Quaderni Costituzionali, Rassegna, 10/2013, 3.*

[286] Sul punto si veda ITALIA, *Libertà e segretezza della corrispondenza e delle comunicazioni,* Milano, 1963, 63.

[287] L'espressione è di CARUSO, *La libertà e la segretezza delle comunicazioni nell'ordinamento nazionale, cit., 4.*

[288] In realtà, siffatta esegesi dell'art. 15 Cost. che rinviene due situazioni giuridiche soggettive nella nozione costituzionale di comunicazione non è accolta in senso unanime in dottrina. Secondo una diversa impostazione, l'art. 15 Cost. predisporrebbe la tutela di «una sola situazione giuridica soggettiva» coincidente con la «libertà delle comunicazioni materialmente assoggettabili e concretamente assoggettate a vincolo di segretezza». In tal senso, ha circoscritto il sistema di tutele predisposte dalla disposizione in esame alle sole comunicazioni sottratte alla conoscibilità dei terzi con le cautele disponibili al mittente PACE, *Art. 15 Cost*., in BRANCA (a cura di), *Commentario della costituzione, Art. 13-20 – Rapporti Civili*, Bologna-Roma, 1977, 85; IBIDEM, *Problematica delle libertà costituzionali. Parte generale*, PADOVA, 2003, 174.

[289] Così CARETTI, BARBIERI, *I diritti fondamentali: Libertà e diritti sociali*, Torino, 2017, 345.

Una volta delineate le linee essenziali della libertà in esame, è necessario analizzare in che modo la conservazione e l'acquisizione di dati di traffico interferisca con essa.

In realtà, la riconducibilità della c.d. *data retention* alla sfera applicativa dell'art. 15 Cost. è stata a lungo dibattuta, complice la formulazione letterale "aperta"[290] della norma da parte dei Padri costituenti[291]. Se infatti la disposizione di rango fondamentale predispone espressamente la tutela della corrispondenza epistolare, il più diffuso mezzo di comunicazione all'epoca dell'entrata in vigore della Costituzione[292], non risultava altrettanto facile capire quali altri strumenti potessero essere inclusi nella categoria "aperta" «ogni altra forma di comunicazione»[293]. In particolare, ci si domandava se i nuovi mezzi di comunicazione interindividuale forniti dallo sviluppo della telefonia digitale rappresentassero una modalità idonea a garantire, dal punto di vista tecnico, un canale ad «accesso riservato»[294], veicolando flussi di dati entro un'area giuridica protetta da riservatezza.

Per la risoluzione della questione, ha giocato un ruolo fondamentale la storica sentenza emanata dalla Corte Costituzionale l'11 marzo 1993, n. 81[295]. Oltre ad aver portato a compimento il percorso interpretativo in materia di intercettazioni avviato nel 1973[296], in tale sede, il Giudice delle leggi si è fatto portavoce di una lettura

---

[290] Grazie a tale clausola di apertura, il paradigma costituzionale *de quo* può ricomprendere, senza la necessità di ricorrere a forzature eccessive della lettera della norma, i mezzi di comunicazione comparsi successivamente alla formulazione della stessa. Così osserva OROFINO, *La libertà di espressione tra Costituzione e Carte europee dei diritti. Il dinamismo dei diritti in una società in continua formazione*, Torino, 2014, 126.

[291] A livello sovranazionale, ha sottolineato l'accezione "ampia" del termine "corrispondenza" la Corte EDU nella sent. Klass ed altri c. Repubblica federale tedesca, 6 settembre 1978.

[292] In origine, la libertà e la segretezza della corrispondenza attribuiva al singolo la pretesa che il contenuto di una epistola restasse segreto rispetto a terzi. Per un approfondimento sulle origini di tale diritto fondamentale si veda CARUSO*, La libertà e la segretezza delle comunicazioni nell'ordinamento nazionale, cit., 2.*

[293] Cfr. ILLUMINATI, Libertà e segretezza della comunicazione, in AA. VV. *Diritti della persona e nuove sfide del processo penale. Atti del XXXII convegno nazionale* (Salerno, 25-27 ottobre 2018), Milano, 2019, 155.

[294] L'espressione è di BRUNO, *Intercettazioni di comunicazioni o conversazioni,* in *Digesto delle discipline penalistiche*, Torino, 1993, 178 e ss.

[295] Per un approfondimento sul contesto di riferimento e sul contenuto della sentenza si veda Cap I § 2.

[296] Si fa riferimento alla celebre sentenza della C. cost. 6 aprile 1973, n. 34, in *Giur. cost.*, 1973, 316, con nota di GREVI, *Insegnamenti, moniti e silenzi della Corte Costituzionale in tema di intercettazioni telefoniche.* Oltre a fissare una serie di punti fermi in materia di intercettazioni telefoniche, la sentenza interpretativa di rigetto ha evidenziato l'esigenza di raggiungere un punto di equilibrio tra la libertà e la segretezza della corrispondenza e l'interesse pubblico alla repressione dei reati. Tutto ciò prima che il parametro di proporzionalità come principio generale si affermasse soprattutto a livello europeo, come sì vedrà in seguito. Cfr. Cap. II § 9.

evolutiva dell'articolo 15 Cost[297]. Pur senza fornire una definizione accurata del concetto di «comunicazione»[298], si è affermato che la norma in esame ricomprende il diritto dell'individuo di scegliere liberamente «il mezzo di corrispondenza, anche in rapporto ai diversi requisiti di riservatezza che questo assicura sia sotto il profilo tecnico, sia sotto quello giuridico»[299]. Pertanto, si è giunti a ricondurre nell'ambito di applicazione della norma le conversazioni effettuate tramite telefono cellulare.

Sulla base di tali premesse, coloro i quali instaurano un flusso di comunicazione mediante utenza mobile hanno il diritto che sia mantenuto segreto non solo il contenuto dello scambio, ma anche i dati "esteriori" attinenti alla conversazione effettuata (identità dei soggetti, tempo e luogo della comunicazione effettuata *etc. etc.*). Secondo la Corte, la *ratio* di tale approdo esegetico si rinviene nello stretto legame sussistente tra il diritto alla riservatezza delle comunicazioni e la «protezione del nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali». Tale nesso comporta «un particolare vincolo interpretativo, diretto a conferire a questa libertà un significato espansivo»[300]. Il rilievo che, sul piano assiologico, la libertà e la segretezza della corrispondenza costituiscono un aspetto inviolabile della persona funzionale al suo svilupparsi in armonia con il principio della "dignità umana"[301], ha portato, dunque, il Giudice delle leggi ad interpretare l'art. 15 Cost. in modo tale da ricomprendere estensivamente tutti i profili relativi all'avvenuta comunicazione.

Una volta riconosciuto che le informazioni relative al fatto storico della conversazione telefonica rientrino nella garanzia accordata dall'articolo sopracitato, la Corte ha verificato in che modo l'attività di acquisizione degli stessi realizzi una

---

[297] Si veda in tal senso anche POTETTI, *Corte Costituzionale n.81/1993: la forza espansiva della tutela accordata dall'art. 15 comma 1 della Costituzione*, in *Cass. Pen.*, 1993, 2746.
[298] ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, *cit.*, 41.
[299] Cfr. Corte Cost., sent. 11 marzo 1993, n. 81, *cit.*, 738.
[300] La Corte Costituzionale, già nella sent. 6 aprile 1973, affermava che l'articolo 15 Cost. trovasse protezione nell'articolo 2 relativo ai diritti inviolabili della personalità.
[301] Siffatta connessione rispetto al valore della "dignità umana" emerge altrettanto chiaramente nei lavori preparatori della Costituzione. La libertà e segretezza della corrispondenza al pari della libertà di domicilio prevista all'art. 14 erano considerati corollari e specificazioni del fondamentale principio dell'inviolabilità della persona umana previsto dall'articolo 13. Il nesso indissolubile che lega l'articolo in commento con gli artt. 13 e 14 rappresenta, inoltre, un elemento a favore dell'adozione di una lettura teleologico-soggettiva della libertà e segretezza delle comunicazioni. Siffatto diritto fondamentale tutela la proiezione spirituale della persona e offre naturale completamento alla garanzia della libertà in senso fisico (art. 13 Cost.) e spaziale (art. 14 Cost.). Più diffusamente sul punto, si veda CARUSO, *La libertà e la segretezza delle comunicazioni nell'ordinamento nazionale*, *cit.*, 4.

compressione del diritto fondamentale in oggetto. Sul punto, la Consulta ha sostenuto che l'attività di *data retention* realizza un'interferenza "attenuata", a differenza di altre metodologie di indagine, tra cui le intercettazioni, considerate di gran lunga più invasive. La Consulta, infatti, delineava un modello di tutela della segretezza delle comunicazioni abbastanza complesso, che si può comprendere in modo più efficace attraverso la c.d. "metafora delle sfere" (o *Sphärentheorie*), introdotta dalla giurisprudenza tedesca[302].

Secondo tale approccio, il valore costituzionalmente garantito dall'articolo 15 può essere paragonato ad una sfera, all'interno della quale si ha un nucleo duro di guarentigie sostanziali e processuali, volto a tutelare la riservatezza del contenuto della comunicazione. Man mano che ci si allontana dal centro della sfera, il medesimo diritto si indebolisce e diviene oggetto di una tutela graduata. Maggiore è la distanza rispetto al nucleo centrale, meno severe devono essere le condizioni imposte alle autorità pubbliche competenti per procedere alla compressione del bene giuridico tutelato[303].

In base a tale impostazione, la Corte osservava che la disciplina delle intercettazioni[304], le quali realizzano una compressione della segretezza del "contenuto" della comunicazione, dovesse prevedere requisiti stringenti; *a contrario*, per limitare la riservatezza dei dati esteriori ai flussi telefonici, si riteneva sufficiente un regime di garanzie meno stringente[305]. In conclusione, il Giudice delle leggi inquadrava la riservatezza dei dati di traffico come un bene giuridico "periferico" [306] rispetto al nucleo centrale coincidente con il contenuto del fatto comunicativo.

Al giorno d'oggi, siffatto indirizzo ermeneutico della giurisprudenza di legittimità appare anacronistico e non condivisibile[307]. Non si comprende, infatti, per quale ragione l'identico valore della segretezza delle comunicazioni, considerato inviolabile dalla Costituzione, debba essere oggetto di tutela differenziata. Altrettanto

---

[302] Sulla *Sphärentheorie* si veda ADDIS, *Diritto all'autodeterminazione informativa e processo penale in Germania*, in AA. VV., *Protezione dei dati personali e accertamento penale*, (a cura di) NEGRI, Roma, 2007, 91.

[303] In tal senso si veda NEGRI, *Compressione dei diritti di libertà e principio di proporzionalità*, in AA. VV. *Diritti della persona e nuove sfide del processo penale. Atti del XXXII convegno nazionale* (Salerno, 25-27 ottobre 2018), Milano, 2019.

[304] Per un approfondimento sulla differenza tra la conservazione dei dati di traffico e le intercettazioni si veda Cap. I §5.1.

[305] Per tale ragione, la Corte riteneva sufficiente l'emanazione di un decreto motivato da parte del pubblico ministero per procedere all'acquisizione di tali dati. Si rimanda sempre al Cap. I § II.

[306] L'espressione è di CONTI, *L'attuazione della direttiva Frattini*, *cit.*, 5.

[307] ANDOLINA, *L'acquisizione nel processo penale*, cit., 46.

irragionevole agli occhi della dottrina recente[308] appare considerare due forme di intrusione nella sfera privata, nella specie le intercettazioni e l'acquisizione dei tabulati di traffico, come «categorie disomogenee»[309]. Nonostante sussistano alcune differenze di natura sostanziale e processuale tra i due mezzi di ricerca della prova[310], le innovazioni tecnologiche hanno contribuito ad assottigliare sempre di più il divario tra i due istituti.

È già stato ampiamente sottolineato che gli sviluppi tecnico-scientifici hanno aumentato la "potenzialità divulgativa" dei dati di traffico telematico sulla personalità dell'utente. In tempi recenti, mediante le informazioni apparentemente "esterne" alla comunicazione è possibile ricostruire le relazioni personali e sociali, orientamenti politici e religiosi, preferenze sessuali e stato di salute della persona a cui si riferiscono[311]. Diventa, dunque, difficile mantenere un rigido *discrimen* tra ciò che attiene al "contenuto" della comunicazione e ciò che invece si limita a fornirne elementi esteriori, collocandola nel tempo e nello spazio.

Tale difficoltà si ripercuote sull'individuazione della modalità di acquisizione delle informazioni suddette. Soltanto laddove non vi sia il rischio che queste rientrino nel "contenuto" della conversazione, sarà possibile predisporre la c.d. *data retention*; in caso contrario, sarà necessario rispettare tutte le garanzie proviste in materia di intercettazioni.

In proposito, si è a lungo dibattuto se i nomi dei siti visitati[312] da un determinato utente rientrino o meno nella nozione di dati "esterni" alla comunicazione. In base alle

---

[308] ILLUMINATI, *Libertà e segretezza della comunicazione*, *cit.*, 155. In senso analogo, CARUSO*, La libertà e la segretezza delle comunicazioni,* cit., 2.

[309] Cfr. Cass., Sez. un., 23 febbraio 2000, n.6, D'Amuri, *cit.* Nel procedimento citato, si è affrontata la questione dell'ammissibilità del sequestro di corrispondenza e delle intercettazioni nei confronti dei detenuti. Tra le varie tematiche che sono state approfondite dalla Corte, si è ribadito il riconoscimento del diritto fondamentale *ex* art 15 Cost. anche in capo ai detenuti.

[310] L'argomento è stato già affrontato nel Cap I § 5.1.

[311] Così si è espresso il Garante della *Privacy* nel Comunicato del 24 gennaio 2008. Si veda *nota successiva*.

[312] L'*Internet Protocol Address* o indirizzo IP è un codice numerico usato da tutte le utenze mobili (*computer*, *server web* etc. etc.) per navigare su *Internet.* Gli indirizzi IP non contengono dati sensibili, tuttavia tramite gli stessi è possibile risalire al *provider* del servizio elettronico prescelto e determinare in maniera più o meno precisa la posizione dell'utente. Rientrano in tale categoria le pagine *web* visitate dall'utente e gli indirizzi IP di destinazione. L'opportunità di estendere, per finalità di indagine, anche agli *Ip adress* l'obbligo di conservazione è una questione ampiamente dibattuta in dottrina. Il dettato letterale dell'art 3 del d.lgs. 109/2008, depone in senso contrario. Se da un lato fa esplicito riferimento agli *Ip* (*Internet Protocol*) di "origine", e cioè quelli che consentono di individuare la fonte della comunicazione, dall'altro non menziona gli *Ip address*, cioè gli indirizzi successivamente visitati dall'utente nel corso della connessione. Tali informazioni risultano soltanto apparentemente "esterne",

precedenti osservazioni, è evidente che soltanto laddove i *website* siano riconducibili a tale categoria, potrebbero essere oggetto di *data storage* ai sensi dell'art. 132 del Codice *Privacy*. Sul punto, si è espresso il Garante nel gennaio 2008, intervenendo a tutela degli utenti di alcune tra le più diffuse compagnie di telefonia sul territorio nazionale. Con il Comunicato stampa del 24 gennaio 2008[313], si è imposto a *Telecom Italia, Vodafone*, *H3G e Wind*, la cancellazione di informazioni detenute illegittimamente che includevano i siti *Internet* visitati dagli utenti.

Una volta affermato che il principio della riservatezza delle comunicazioni trovi applicazione anche durante la navigazione in *Internet* e nell'uso dei motori di ricerca, il Garante ha affermato che i gestori telefonici non possono archiviare tali informazioni nemmeno per esigenze di giustizia. I fornitori di servizi telefonici e telematici devono infatti limitarsi a conservare esclusivamente i dati di traffico. Sono esclusi da tale categoria i dati apparentemente esterni alla comunicazione, ma che di fatto coincidono con il loro contenuto, permettendo di ricostruire la personalità e le relazioni sociali dell'utente a cui si riferiscono[314].

Sulla base di tali premesse, si ordinava alle compagnie telefoniche sopracitate la cancellazione entro due mesi di tutte le informazioni raccolte durante la navigazione compresi gli indirizzi *IP* dei siti *Internet* visitati dagli utenti e «le interrogazioni ai motori di ricerca». Inoltre, veniva vietato l'utilizzo di sistemi informatici (*proxy*

---

in quanto sono in grado di rivelare di fatto anche il contenuto della navigazione (c.d. *on line content information*). Per tale ragione, sono escluse dal novero dei dati passibili di conservazione da CONTI, *L'attuazione della direttiva Frattini*, *cit.*, 15. *A contrario*, sottolineano l'estrema utilità nel contrasto ai crimini perpetrati per mezzo di *Internet* e sono più inclini ad ammetterne la conservazione CAJANI, *Investigazioni vs.* privacy: *il bilanciamento di opposti interessi.* in AA.VV. Computer forensics *e indagini digitali. Manuale tecnico giuridico e casi pratici, Vol. I*, Forlì, 2011, 333 ss.; ATERNO, CISTERNA, *Il legislatore interviene ancora sulla* data retention*, ma non è finita*., in *Dir. Pen. e proc*., 2009, 293 ss.
In giurisprudenza, in casi di ingiuria e diffamazione realizzati per mezzo della posta elettronica, si è ammessa l'utilizzabilità degli *Ip address* dell'utenza telefonica di trasmissione (cfr. Cass. Pen. Sez. V, 10 Marzo 2010, n. 19491 in CED n. 2473109).

[313] Si tratta del doc. web n. 1481285, consultabile *online* in *www.garanteprivacy.it.*

[314] Sul punto si veda quanto affermato da un componente del Garante della *Privacy* italiano, PAISSAN: «Questi provvedimenti affermano un principio innovativo e importante: va tutelata la riservatezza anche della navigazione in *Internet* e dell'uso dei motori di ricerca. I gestori telefonici non possono dunque conservare questi dati nemmeno per ragioni di giustizia. Entro due mesi queste informazioni dovranno ora scomparire. Viene in questo modo riaffermata l'estrema delicatezza delle visite e delle ricerche in *Internet*».

server[315]), non necessari per la fornitura dei servizi né per operazioni di fatturazione, che invece consentono una ingente raccolta di dati relativi alla connessione in rete.

Tale episodio, ormai risalente a più di una decina di anni fa, dimostra quanto si sia gradualmente ampliato l'angolo di incidenza dell'articolo 15 della Costituzione. In primo luogo, l'oggetto di tutela della norma si estende a qualunque forma di comunicazione privata, indipendentemente dal mezzo utilizzato dall'utente, tale da assicurare almeno «convenzionalmente, secondo aspettative obiettivamente ragionevoli» la segretezza del messaggio trasmesso[316]. Sono sottoposti alla tutela prevista dal paradigma normativo sopracitato tutti i mezzi di comunicazione comparsi successivamente alla stesura del testo costituzionale, compresi quelli che trasmettono flussi digitalizzati tramite sistemi VOIP[317] o sulle piattaforme dei *social network*.

In secondo luogo, alla segretezza del messaggio trasmesso si affianca quella relativa alle informazioni "esterne" che ad esso riferiscono[318]. Ricadono, dunque, nella nozione estesa di comunicazione, in quanto espressioni "divulgative" della personalità dell'utente, *inter alios*, il numero telefonico, l'ora e la durata della conversazione e le celle telefoniche agganciate. Pertanto, anche nei confronti di siffatti dati è necessario che siano rispettati i presidi di salvaguardia della sfera individuale previsti dall'articolo 15 Cost., comma 2.

2.1 La riserva di legge prevista dall'art. 15 della Costituzione.

Tale disposizione prevede un doppio meccanismo di tutela, perché basato sia sulla riserva di legge sia su quella di giurisdizione[319]. In base al primo requisito, è possibile disporre una misura che limiti il valore della libertà e della segretezza delle comunicazioni «soltanto per atto motivato dell'autorità giudiziaria con le garanzie

[315] In ambito informatico, il *Proxy* indica un tipo di server, che, interponendosi tra l'utente e il sito a cui si richiede l'accesso, funge da intermediario per le richieste da parte dei clienti. Una volta ricevuta la richiesta del cliente (ad esempio di un *file* o di una pagina *web*), quest'ultimo la valuta e la esegue.

[316] Cfr. PACE, Problematica delle libertà costituzionali, cit., 248. L'Autore sottolinea che non possa pretendersi «l'assoluta impossibilità tecnica dei terzi di impedire la comunicazione del messaggio o di captarne il contenuto» perché altrimenti «l'ambito di applicazione dell'articolo 15 cost. sarebbe praticamente nullo, a fronte delle sofisticatissime risorse che la odierna tecnologia mette a disposizione di quanti intendono impedire o captare le altrui comunicazioni».

[317] Per la definizione di VOIP si faccia riferimento a Cap I § 4.3 (*nota* 126).

[318] La segretezza dei dati "esterni" non opera soltanto nei confronti dei fornitori di servizi telefonici telematici che, *ratione officii*, ne entrano inevitabilmente a conoscenza, pur essendo obbligati a mantenere il completo riserbo. Sul punto si veda OLIVETTI, *Brevi note in materia di libertà di comunicazione*, in *Giur. Cost*., 1996, 3858.

[319] Sottolinea come la doppia riserva di legge e di giurisdizione rappresenti lo statuto ordinario di tutela dei diritti soggettivi BARILE, CHELI, *Corrispondenza (libertà di)*, cit., 749.

stabilite dalla legge». Si tratta di una riserva di legge assoluta[320], in quanto esclude l'intervento di fonti *sub*-legislative dalla disciplina della materia[321]. Ne consegue che le misure restrittive della libertà di comunicazione devono essere integralmente previste dalla legge formale ordinaria o da atti ad essa equipollenti[322], salvo i regolamenti di stretta esecuzione[323].

La *ratio* di una riserva così stringente è facilmente riconducibile al fatto che le libertà fondamentali sono naturalmente rivendicate contro il potere coercitivo dello Stato[324]. È, dunque, precluso agli organi governativi prevedere limitazioni a suddetti diritti mediante l'emanazione di fonti regolamentari ed esecutive, imponendo il rispetto delle garanzie che la legge comporta.

Proseguendo con l'esegesi dell'art. 15 Cost, in dottrina si è dibattuto a lungo se l'inciso «con le garanzie stabilite dalla legge» rappresenti un *quid pluris* rispetto all'espressione «nei casi e nei modi stabiliti dalla legge» prevista dagli articoli 13[325] e 14[326] Cost. Secondo una lettura sistematica delle norme in esame, la legge non si dovrebbe limitare a prevedere le condizioni in base alla quali la libertà e la segretezza delle comunicazioni possano essere legittimamente compresse. Sarebbe invece

---

[320] La distinzione tra riserva assoluta e riserva relativa è stata da tempo recepita dalla Corte costituzionale (*ex plurimis*, si vedano le sentenze n. 4/1957, 30/1957 e 26/1966) e dal legislatore ordinario (cfr. art 17 l. 400/1988). Sulla base di tale distinzione, è ormai orientamento consolidato in dottrina che gli articoli 13, 14 e 15 della Costituzione prevedano riserve assolute in quanto riguardino materie completamente sottratte al potere dell'esecutivo. Sul punto si veda CARUSO, *La libertà e la segretezza delle comunicazioni nell'ordinamento nazionale*, *cit.*, 9; SALERNO, *La protezione della riservatezza e l'inviolabilità della corrispondenza"* in NANIA (a cura di), *I diritti costituzionali,* Torino, 2001.

[321] Inoltre, la riserva di legge dell'art. 15 Cost. non è da intendersi solo come statale. In conformità con l'articolo 117, comma 2, lett. *l)* Cost. siffatta materia non è attribuita alla competenza esclusiva dello Stato, ragion per cui potrebbe essere disciplinata anche da leggi regionali.

[322] Si tratta infatti di una riserva di legge non meramente formale in quanto, oltre alle leggi approvate dal Parlamento, sono incluse tra le fonti normative tutti gli atti ad essa equivalenti, e cioè i decreti legislativi e i decreti-legge. Sul punto si veda BALDUCCI, *Le garanzie nelle intercettazioni tra costituente e legge ordinaria*, Milano, 2002.

[323]Sottolinea come sia da escludere espressamente l'intervento di fonti normative regolamentari UBERTIS, *I diritti fondamentali nel processo penale, in Sistema di procedura penale. Principi generali*, vol. I, Milano, 2017, 240.

[324] Cfr. BIN, PITRUZZELLA, *Diritto costituzionale,* Torino, 2020, 356.

[325] Si ritiene utile riportare i commi 1 e 2 dell'articolo 13 Cost. nella loro interezza:
«La libertà personale è inviolabile.
Non è ammessa forma alcuna di detenzione, di ispezione o perquisizione personale, né qualsiasi altra restrizione della libertà personale, se non per atto motivato dell'autorità giudiziaria e nei soli casi e modi previsti dalla legge».

[326] L'art 14 Cost. dispone che:
«Il domicilio è inviolabile.
Non vi si possono eseguire ispezioni o perquisizioni o sequestri, se non nei casi e modi stabiliti dalla legge secondo le garanzie prescritte per la tutela della libertà personale».

compito del legislatore ordinario individuare anche specifiche modalità e cautele finalizzate a contemperare *ex ante* il potenziale contrasto tra il diritto fondamentale tutelato e l'interesse generale a perseguire i reati[327].

Dopo aver individuato ai sensi dell'articolo 13 Cost. le tipologie di reati gravi che legittimerebbero una deroga al principio della segretezza delle comunicazioni, la legge dovrebbe, dunque, prevedere ulteriori garanzie che predispongano una tutela aggiuntiva ai titolari del rapporto comunicativo[328]. In sintesi, secondo tale approccio, "i casi e i modi" previsti agli articoli 13 e 14 e le "altre garanzie" dell'art. 15 Cost. dovrebbero essere considerati congiuntamente e non in antinomia[329].

2.2 La riserva di giurisdizione.

Ai sensi dell'art. 15 Cost. è poi prevista la riserva di giurisdizione[330], che rappresenta un ulteriore vincolo all'attività dei poteri pubblici in materia di libertà fondamentali. In questo modo, ogni atto che incide sulla segretezza delle comunicazioni non solo deve essere previsto "in astratto" dalla legge, ma è necessario che sia autorizzato "in concreto" dal giudice «per atto motivato dell'autorità giudiziaria»[331].

Inoltre, a differenza di quanto dispongono gli articoli 13[332] e 14 Cost.[333], non è previsto il riconoscimento di poteri sostitutivi o provvisori in capo alle autorità di

---

[327] Tale lettura sistematica non è, però, condivisa all'unanimità in dottrina. Si vedano in senso contrario BARILE, CHELI, *Corrispondenza (libertà di)*, cit., 749. Gli autori sostengono che l'espressione «nei casi e nei modi stabiliti dalla legge» contenuta negli artt. 13 e 14 Cost. avrebbero lo stesso significato del sintagma «con le garanzie stabilite dalla legge» previsto dall'art. 15 Cost.

[328] Sul punto, si veda CARUSO, *La libertà e la segretezza delle comunicazioni,* cit., 9.

[329] Questo sembra essere l'approccio seguito nel codice di procedura penale, in cui, all'articolo 266, il legislatore predispone un elenco tassativo dei singoli tipi di reato per cui è possibile procedere alle intercettazioni telefoniche.

[330] Accanto alla riserva di giurisdizione vi sono tutta una serie norme sul giusto processo nel c.p.p. che, pur non coincidendo con il contenuto proprio della riserva, contribuiscono a renderla effettiva. V. PACE, *Problematica delle libertà costituzionali*, cit., 174.

[331] Il requisito della riserva di giurisdizione accomuna tutta una serie di diritti fondamentali attinenti sia alla sfera personale sia alla sfera pubblica e sociale dell'individuo. Sul punto, si vedano, infatti, oltre all'articolo 15 sopracitato, gli articoli 13, comma 2, 14, comma 2, 21, comma 3 e 4.

[332] Secondo l'art. 13, comma 3, della Costituzione:
«In casi eccezionali di necessità ed urgenza, indicati tassativamente dalla legge l'autorità di pubblica sicurezza può adottare provvedimenti provvisori, che devono essere comunicati entro quarantotto ore all'autorità giudiziaria e, se questa non li convalida nelle successive quarantotto ore, si intendono revocati e restano privi di ogni effetto». In breve, si dà la possibilità all'autorità di pubblica sicurezza di adottare provvedimenti restrittivi della libertà personale fintanto che subentri l'intervento di convalida dell'autorità giudiziaria entro i quattro giorni successivi.

[333] L'articolo 14, comma 3, della Costituzione prevede che:
«Gli accertamenti e le ispezioni per motivi di sanità e di incolumità pubblica o a fini economici e fiscali sono regolati da leggi speciali».

pubblica sicurezza che possono essere utilizzati in casi di necessità e urgenza. Sul punto, il Costituente ha dunque adottato uno statuto di tutela rafforzato rispetto a quello previsto per la libertà personale e domiciliare, riconoscendo all'autorità giudiziaria una competenza esclusiva.

La scelta dell'Assemblea Costituente di non prevedere poteri di intervento in capo alle autorità di pubblica sicurezza appare fondata sul precipuo contenuto della libertà in esame che la distingue dagli altri diritti fondamentali della persona. Contrariamente alle misure previste per la libertà personale o di domicilio, le limitazioni che incidono sulla segretezza delle comunicazioni coinvolgono sempre «un altro soggetto, sia esso l'interlocutore telefonico, il mittente o il destinatario di una lettera»[334]. L'intervento provvisorio degli organi di polizia, in attesa di quello della magistratura, avrebbe, dunque, maggiore possibilità di arrecare un danno ad una pluralità di individui inevitabilmente coinvolti. Per tale ragione, la scelta rigorosa del Costituente sembra essere ben meditata e ragionevole[335].

Quanto all'espressione «autorità giudiziaria» dell'art. 15 Cost., il dato letterale sembrerebbe ricomprendere in astratto, tra i soggetti che possono predisporre misure restrittive della libertà di comunicazione, anche il pubblico ministero. Eppure, sul punto la dottrina prevalente[336] si è orientata nel senso di adottare una interpretazione restrittiva della locuzione in esame, che includesse soltanto la figura dell'organo giudicante. L'esigenza di incrementare le salvaguardie che contraddistinguono la tutela della segretezza è dovuta a molteplici ragioni.

In primo luogo, vengono in rilievo una serie di elementi letterali, tra cui l'analogia con l'articolo 13 Cost., commi 2 e 3, in cui si rinviene la medesima espressione, spesso interpretata in senso restrittivo come "autorità giurisdizionale". Inoltre, in coerenza con l'impostazione accusatoria[337] del nostro codice di rito penale, l'articolo 111, comma 7, che sancisce il principio costituzionale del «giusto processo»,

---

[334] Si tratta dell'orientamento prevalente in dottrina. In tal senso BRUNO, *Intercettazioni di comunicazioni o conversazioni, cit*., 181; BALDUCCI, *Le garanzie nelle intercettazioni*, cit., 2002, 45; CAMON, Le intercettazioni, *cit*., 3. *A contrario*, si è espresso in senso critico a tale ricostruzione, criticando la scelta di prevedere all'articolo 15 Cost. una disciplina più rigorosa rispetto agli artt. 14 e 13 BARILE, CHELI, *Corrispondenza (libertà di)*, *cit.*, 749.

[335] Cfr. PACE, *Art. 15 Cost*., cit., 106.

[336] *Inter alios*, optano per una più stringente interpretazione della locuzione «autorità giudiziaria» BALDUCCI, *Le garanzie nelle intercettazioni*, cit., 2002, 45; BRUNO, *Intercettazioni di comunicazioni o conversazioni,* cit., 188; CAMON, *Le intercettazioni*, cit., 109.

[337] Per un approfondimento sul punto si rinvia al Cap. III.

prevede che i «provvedimenti sulla libertà personale sono pronunciati dagli organi giurisdizionali».

In secondo luogo, il dibattito attorno all'esegesi di siffatta espressione è stato alimentato dalla disomogeneità degli interventi normativi in materia. Da un lato, il legislatore ha infatti riservato il potere di autorizzare le intercettazioni al giudice delle indagini preliminari[338]; dall'altro, ha individuato in capo al pubblico ministero la competenza esclusiva di acquisire i dati di traffico telefonico e telematico[339]. Nonostante, si tratti in entrambi i casi di misure che incidono sulla sfera inviolabile della persona, il legislatore ha, dunque, dato attuazione in modo differenziato al riferimento all'autorità giudiziaria contenuto all'art. 15 Cost.

Sotto tale profilo, il potere del pubblico ministero di disporre, in via autonoma e senza l'intervento autorizzativo dell'organo giurisdizionale[340], della c.d. *data retention* per finalità di indagine, rappresenterebbe una netta regressione dello statuto di tutela della sfera privata. Soprattutto dinnanzi alla elevata potenzialità intrusiva e divulgatrice dello strumento in esame, non si capisce per quale ragione si siano predisposte garanzie processuali meno stringenti rispetto a quelle esistenti per altri strumenti di ricerca della prova, *sub specie* le intercettazioni[341].

In conclusione, la disciplina attualmente vigente in materia di acquisizione dei tabulati telefonici risulta in contrasto con le garanzie processuali predisposte dall'articolo 15, comma 2, della Costituzione, interpretate alla luce del dato sistematico. Inoltre, il riconoscimento in capo all'organo di accusa di un potere coercitivo del tutto svincolato dal diretto controllo dell'autorità giurisdizionale stride con il ruolo di parte processuale da questi ricoperto. Mediante l'attribuzione di una

---

[338] Si fa riferimento all'art. 267 c.p.p. che dispone i «presupposti e le forme del provvedimento» di autorizzazione delle intercettazioni. Secondo tale articolo: «Il pubblico ministero richiede al giudice per le indagini preliminari l'autorizzazione a disporre le operazioni previste dall'articolo 266. L'autorizzazione è data con decreto motivato quando vi sono gravi indizi di reato e l'intercettazione è assolutamente indispensabile ai fini della prosecuzione delle indagini». Sulla disciplina delle intercettazioni si veda anche Cap I § 5.1.

[339] In realtà, come si visto nel. Cap 1 §4.3 e 4.4 a cui si rinvia, il P.M. non ha il monopolio assoluto dell'acquisizione dei tabulati telefonici. L'articolo 132, comma 3, del Codice *Privacy* prevede infatti la possibilità in capo al difensore dell'imputato o della persona sottoposta alle indagini di rivolgersi direttamente al gestore del servizio di comunicazione per l'acquisizione dei tabulati relativi al proprio assistito. Si tratta però di un potere di acquisizione assai limitato e residuale.

[340] Si veda il tal senso l'art. 132 del Codice *Privacy*. Per un approfondimento sul procedimento di acquisizione dei tabulati Cfr. Cap. I §4.3.

[341] Cfr. ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, *cit.*, 114.

competenza esclusiva, o quasi[342], in capo al P.M.[343] si mette infatti a rischio il principio di "parità delle parità"[344], imprescindibile corollario del «giusto processo» ai sensi dell'articolo 111, comma 2, Cost.

3. L'inviolabilità del domicilio ai sensi dell'art. 14 della Costituzione: un'interpretazione evolutiva del dato normativo.

Come si è anticipato, l'attività di acquisizione dei dati telefonici e telematici rappresenta il crocevia di una serie di diritti e libertà individuali che si intersecano tra di loro. Oltre alla segretezza delle comunicazioni, la c.d. *data retention* viene ad interferire con l'inviolabilità del domicilio ai sensi dell'articolo 14 della Costituzione[345]. La peculiare capacità intrusiva di tale metodica di indagine, infatti, non solo incide sulla tutela del contenuto e delle informazioni "esterne" all'atto comunicativo, ma produce un'inevitabile intromissione nella dimensione spaziale attraverso la quale si estrinseca la personalità del singolo.

In base a quanto detto *supra*[346], si è rilevato che, attraverso l'acquisizione di un tabulato che si riferisca ad una utenza "mobile"[347], si è in grado di individuare il luogo in cui si trovava il soggetto nel momento in cui ha usufruito del servizio di comunicazione elettronica[348]. Ciò in quanto un apparecchio telefonico che si sposta nello spazio deve rinegoziare la connessione con la rete telefonica dalla cella – *rectius*, torre radio – agganciata durante la sua posizione iniziale a quella che ricopre la sua

[342] Si fa qui riferimento all'acquisizione dei tabulati di traffico telefonico su richiesta del difensore ai sensi dell'art. 132, comma 3, del Codice *Privacy*. Cfr. Cap. I § 4.4.
[343] Si è visto, in realtà, di come si tratti di una competenza "semi-esclusiva" in quanto il difensore può acquisire i tabulati del traffico telefonico del proprio assistito ai sensi dell'art. 132, comma 3, del Codice *Privacy*. Cfr. Cap. I §4.4.
[344] Il tema verrà trattato ampliamente nel Cap III.
[345]La disposizione costituzionale è stata riportata integralmente nella nota 43, a cui si rinvia.
[346] Si fa riferimento al Cap. I § 5.5.
[347] Per una definizione di utenza "mobile" si veda Cap. I § 1 *nota* 3.
[348] Sul punto si è espressa la Corte cost. 28 maggio 2010, n. 188, consultabile in *www.cortecostituzionale.it*. Il procedimento *de quo* ha ad oggetto il conflitto di attribuzione tra poteri dello Stato sorti a seguito del diniego da parte del Senato di autorizzare l'utilizzo dei tabulati telefonici acquisiti nei confronti di un senatore. Nella sentenza, la Consulta ha ribadito la «notevole capacità intrusiva generalmente riconosciuta» alla c.d. *data retention*, richiamando il formante giurisprudenziale in materia (Cfr. sentenze della Corte Cost. n. 372 del 2006, n. 281 del 1998 e n. 81 del 1993). Inoltre, ha sottolineato che «i tabulati consentono di apprendere e individuare non solo tutti i contatti con altre utenze e la loro collocazione temporale, ma – se si tratta di apparecchi mobili – anche il cosiddetto "tracciamento", vale a dire le localizzazioni e gli spostamenti dei soggetti detentori dell'apparecchio». Pertanto, tali informazioni possono aprire «squarci di conoscenza» sui rapporti del soggetto a cui è intestato il telefono.

attuale ubicazione[349]. Tramite la richiesta al gestore del pubblico servizio del tabulato di traffico, l'autorità giudiziaria è dunque in grado di ricostruire i movimenti dell'utenza e, in via mediata, del suo intestatario[350].

Ciò posto, è necessario capire in che modo il "tracciamento" degli spostamenti dell'individuo detentore dell'apparecchio telefonico produca un'interferenza con l'articolo della Costituzione in esame.

In breve, la libertà tutelata dall'articolo 14 della Costituzione si traduce nel potere riconosciuto in capo al singolo di limitare l'ingresso allo Stato e a terzi nel proprio domicilio. L'elemento qualificante l'esercizio di siffatto diritto fondamentale, che rientra le «tradizionali libertà negative»[351], consiste, dunque, nello *ius prohibendi* qualsiasi intrusione di tipo fisico nei luoghi in cui si estrinseca l'intimità della vita privata dell'individuo. Accanto a questa dimensione puramente proibitiva[352], a cui corrisponde la pretesa del singolo di un comportamento omissivo da parte di terzi, rientra nell'ambito di applicazione dell'articolo 14 Cost. anche il diritto di ammettere nel proprio domicilio (*ius admittendi*) altre persone, al fine di realizzare la propria dimensione sociale e affettiva[353].

In questa prospettiva, la *ratio* alla base del meccanismo di tutela accordato al domicilio deve riconoscersi nell'esigenza di riservatezza di accordare il diritto di escludere e allo stesso tempo ammettere altre persone dai luoghi in cui si svolge la "vita intima" di ciascun individuo. Questo approccio esegetico, che accorda alla libertà di domicilio una latitudine estesa, pone in evidenza come la garanzia costituzionale accordata dall'art. 14 Cost. sia una premessa indispensabile per il concreto esercizio

[349]Sul punto si veda DINACCI, *Localizzazione attraverso celle telefoniche*, cit., 371.
[350]Parla del c.d. *positioning* e cioè della collazione del soggetto durante la telefonata, tramite l'aggancio delle celle telefoniche anche MARCOLINI, *L'istituto della* data retention *dopo la sentenza della corte di giustizia del 2014*, cit. 181.
[351]Sul punto si veda SILVESTRI, *L'individuazione dei diritti della persona*, in *Dir. pen. Cont.*, 2018, 1.
[352] Evidenzia come accanto alla tradizionale libertà del domicilio intesa come *ius excludendi alios,* e cioè come pura e semplice «facoltà di proibire l'ingresso a terzi», vi sia anche il c.d. *ius admittendi* PACE, *Problematica delle libertà costituzionali,* cit., 212.
[353]Cfr. Corte Cost., 16 maggio 2008, n. 149, in *Giur. Cost*., 2008, 1825 e ss. Nel procedimento *de quo*, la Corte ha affrontato la questione di legittimità costituzionale dell'art. 266, comma 2, del codice di procedura penale, nella parte in cui non estendeva la disciplina delle intercettazioni tra presenti «a qualsiasi "captazione di immagini in luoghi di privata dimora"». Nella pronuncia, la Consulta ha aderito alla tesi secondo cui l'art. 14 Cost. accorda una duplice tutela alla libertà di domicilio. Sul punto, ha evidenziato che «l'art. 14 Cost. tutela il domicilio sotto due distinti aspetti: come diritto di ammettere o escludere altre persone da determinati luoghi, in cui si svolge la vita intima di ciascun individuo; e come diritto alla riservatezza su quanto si compie nei medesimi luoghi».

delle altre libertà fondamentali[354], tra cui rientrano quelle garantite dagli articoli 13 e 15 Cost.

All'interno di questa ampia cornice costituzionale «il presidio di un'intangibile sfera di riservatezza» può essere leso non solo attraverso un'intrusione di tipo fisico ma anche attraverso l'uso di strumenti tecnici[355] che rendano «visibile a terzi» quanto si svolge nel luogo di privata dimora[356]. Ciò detto, la possibilità di "tracciare" la presenza di persone nel domicilio di un soggetto mediante l'acquisizione dei tabulati di traffico si può dire equivalente a rendere «visibile» ciò che l'individuo aveva il diritto di mantenere riservato[357]. Inoltre, la localizzazione della posizione di un soggetto tramite celle telefoniche consente di verificare se lo stesso abbia preso parte ad un incontro tenutosi in un determinato luogo insieme ad altri soggetti, anch'essi titolari di utenze telefoniche delle quali si sono acquisiti i tabulati.

In conclusione, anche se con minore intensità rispetto ad altre metodologie investigative[358], la conoscenza da parte degli organi inquirenti degli «spostamenti dei soggetti detentori dell'apparecchio»[359] interferisce con il valore dell'inviolabilità del domicilio.

3.1 Il c.d. "domicilio informatico".

Tale interferenza risulta ancora più evidente se si adotta una lettura evolutiva dell'articolo 14 Cost. alla luce di nuove esigenze di tutela emerse a seguito del progredire tecnologico. Il proliferarsi di atti atipici di investigazione[360] idonei ad

---

[354] Cfr. MONTAGNA, *Libertà domiciliare*, in AA. VV. *Diritti della persona e nuove sfide del processo penale. Atti del XXXII convegno nazionale* (Salerno, 25-27 ottobre 2018), Milano, 2019, 120.

[355] Cfr. Corte cost., 16 maggio 2008, n. 149, cit. Sul punto, il Giudice di legittimità ha affermato che l'articolo 14 della Costituzione funge da «presidio di un'intangibile sfera di riservatezza» che «può essere lesa – attraverso l'uso di strumenti tecnici – anche senza la necessità di un'intrusione fisica».

[356] Cfr. Corte cost., 16 maggio 2008, n. 149, cit. Sempre nella medesima sentenza si è affermato che «affinché scatti la protezione dell'art. 14 Cost., non basta che un certo comportamento venga tenuto in luoghi di privata dimora; ma occorre, altresì, che esso avvenga in condizioni tali da renderlo tendenzialmente non visibile a terzi».

[357] Sul punto v. DINACCI, *Localizzazione attraverso celle telefoniche*, cit., 371.

[358] Si fa riferimento attività di indagine che producono un'interferenza manifesta rispetto all'inviolabilità del domicilio. Tra di esse, è opportuno annoverare le ispezioni, le perquisizioni, i sequestri e tutti gli altri mezzi di ricerca della prova che realizzano una intrusione di tipo fisico. Tra le operazioni invasive della libertà domiciliare che non causano una interferenza di tipo fisico, rientrano le videoregistrazioni. Si tratta di riprese visive che gli organi investigativi eseguono all'interno del domicilio, superando una barriera che si frappone tra la generalità dei consociati e l'attività filmata.

[359] Cfr. Corte cost. 28 maggio 2010, n. 188, cit.

[360] Si tratta per lo più di strumenti di sorveglianza *on line* realizzati per il tramite di un virus informatico (c.d. *trojan horse* o captatore informatico) che, una volta introdotto in dispositivi elettronici, è in grado di realizzare operazioni di "captazione da remoto". Siffatta metodologia è altamente invasiva e

incidere sulla sfera privata digitale dell'individuo, ha fatto acquisire alla disposizione costituzionale *de qua* una nuova "dimensione tecnologica" tale da ricomprendere il c.d. "domicilio informatico" o "digitale"[361]. Il concetto *de quo* fa riferimento al luogo virtuale in cui si trovano custoditi una serie di dati e informazioni, tramite i quali si realizza una proiezione integrale della persona nella sua dimensione elettronica[362]. Se il domicilio è il luogo in cui si esprime di diritto la personalità di un individuo, lo «spazio digitale»[363] rappresenta di riflesso una prosecuzione di siffatta sfera intima e privata che deve essere oggetto di analoga protezione da parte dell'ordinamento.

In tal senso, la conservazione e l'acquisizione dei dati di traffico andrebbe a realizzare, dunque, non solo una compressione della libertà domiciliare mediante il tracciamento degli spostamenti del singolo, ma anche un'interferenza rispetto al "luogo" virtuale all'interno del quale l'individuo esprime la propria personalità. Come anticipato, tra le informazioni oggetto di *data retention* rientrano infatti, oltre al numero telefonico del chiamante e i dati necessari per determinare l'ubicazione dell'apparecchio mobile, tutti gli indirizzi *IP* che identificano colui che usufruisce del servizio informatico[364]. Mediante gli stessi, è possibile risalire al tipo di tecnologia adoperata dall'utente e all'operazione da questi effettuata (utilizzo del servizio di posta elettronica, messaggistica via *Internet etc. etc*.). Inoltre, in via mediata, è possibile ricostruire tutte le dinamiche sociali che rientrano nella sfera privata dell'individuo e che contribuiscono a determinarne la personalità. Pur non effettuando un accesso diretto al sistema informatico, gli organi inquirenti entrano in possesso di una serie di

---

sostanzialmente riconducibile alla *c.d.* perquisizione *on line*. L'autorità inquirente è infatti in grado di accedere a tutti i dati informatici (*file* e immagini) contenuti nel dispositivo mobile utilizzato dall'indagato (c.d. *online search*). Vengono inoltre registrati tutti i movimenti all'interno del *web* e ogni attività effettuata mediante il dispositivo sotto controllo (c.d. *online surveillance*). Per una definizione di captatore informatico e un approfondimento sulle nuove metodologie di indagine si veda CUOMO, *La prova digitale*, in CANZIO-LUPÀRIA (a cura di), *Prova scientifica e processo penale*, Milano, 2018, 724.

[361] *Ab origine*, il concetto di c.d. domicilio informatico è stato elaborato nell'ordinamento nazionale in riferimento ai reati informati e, nella specie, al reato di accesso abusivo a un sistema informatico o telematico ai sensi dell'art. 615-*ter* c.p. Tale fattispecie incriminatrice è stata infatti collocata nella sezione IV del Capo II del Titolo XII del codice penale, inerente ai reati contro l'inviolabilità del domicilio. L'art. 615-*ter* c.p. punisce con la reclusione fino a 3 anni coloro che accedono abusivamente ad un sistema informatico, inteso in senso fisico (*personal computer*) oppure virtuale (l'insieme dei dati in esso contenuti).

[362] In tal senso RODOTÀ, *Comunicato Stampa del Garante per la protezione dei dati personali*, 16 settembre 2004, in *www. privacy.it.*

[363] *Inter alios*, sul concetto di domicilio informatico nella dottrina italiana, si v. CAMON, *Cavalli di Troia in Cassazione*, in *Archivio della nuova procedura penale*, 2017, 95.

[364] In proposito si veda Cap. I § 4.1.

informazioni, apparentemente "esterne", ma di fatto rientranti nello "spazio virtuale" da cui si intende escludere gli altri, e cioè in quello che viene definito "domicilio informatico".

In dottrina, ci si è domandato a lungo se la tutela di tale "luogo" dematerializzato sia ascrivibile ad uno dei fondamenti costituzionali preesistenti, *sub specie* a quello predisposto dall'articolo 14 Cost., o se corrisponda ad un "nuovo fondamento"[365]. Non sarebbe infatti la prima volta che dall'ampliamento della protezione offerta da una previsione espressa a livello costituzionale, si verifichi la germinazione di "diritti di nuova generazione"[366] che rispondono ad esigenze di tutela emerse di recente.

A tal riguardo, si sono riscontrati approcci interpretativi disomogenei che hanno portato anche a conclusioni tra di esse discordanti. Da un lato, si è sottolineata l'esigenza di prestare idonea garanzia alla dimensione "virtuale" del domicilio attraverso la costruzione di un diritto inedito[367], dall'altra si è ribadita la possibilità di ricondurre tale aspetto innovativo alla tutela apprestata dall'art. 14 Cost. In base a siffatta lettura evolutiva della norma in discussione[368], l'attenzione andrebbe focalizzata non sul "luogo" in cui si esplica la libertà domiciliare bensì sul conflitto di interessi, pubblici e privati, che la Costituzione mira a tutelare.

Come si è detto poc'anzi, la *ratio* alla base dell'art. 14 Cost. è quella di salvaguardare la sfera "intima" e riservata del singolo che viene proiettata in un

---

[365] Cfr. MONTAGNA, *Libertà domiciliare*, *cit.*, 145.

[366] Ha evidenziato "l'autonoma forza generativa" di nuovi diritti SILVESTRI, *L'individuazione dei diritti della persona*, in AA. VV. *Diritti della persona e nuove sfide del processo penale. Atti del XXXII convegno nazionale* (Salerno, 25-27 ottobre 2018), Milano, 2019, 23. Di seguito, L'Autore ha, però, ribadito che non si tratti di diritti "nuovi" in senso proprio, bensì di valori inclusi implicitamente in quelli espressamente nominati ovvero risultanti dalla composizione di diritti già esistenti.

[367] Di recente, ha aderito a tale impostazione la Corte costituzionale tedesca con la decisione del 20 aprile 2016, *(1BvR 966/09)*. È possibile visionare il testo della sentenza in lingua inglese in *www.bundesverfassungsgericht.de.* La pronuncia è commentata da VENEGONI-GIORDANO, *La Corte Costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici,* in *www.dirittopenalecontemporaneo.it*. In tale sede, i giudici tedeschi hanno negato che la tutela da apprestare per l'uso riservato delle tecnologie informatiche sia rinvenibile nell'art. 13 della Costituzione (*Grundgesetz*) sull'inviolabilità del domicilio. Invece di ricorrere alla tutela offerta dai diritti costituzionali già previsti nella Carta, la Corte ha sottolineato l'esigenza di coniare un "nuovo" diritto fondamentale, mediante il quale garantire al cittadino la tutela di uno spazio "dematerializzato" e "digitale" in cui si estrinseca la sua personalità. Il *Bundesverfassungsgericht* si era già fatto portavoce di tale approccio esegetico nella sentenza del 27 febbraio 2008, di cui verrà fatta menzione nel Cap II §.

[368] A sostegno di siffatta lettura evolutiva v. MONTAGNA, *Libertà domiciliare*, *cit.*, 145.

determinato spazio, dal quale si intende escludere la presenza di terzi[369]. Pertanto, il fatto che si tratti un luogo fisico e chiuso (la dimora) o di uno spazio dematerializzato[370], quale quello virtuale di un dispositivo mobile informatico, non dovrebbe influire sul bene giuridico tutelato dalla norma. Ciò anche in considerazione della stretta connessione tra l'art. 14 Cost. e le garanzie predisposte dagli artt. 13 e 15, che apprestano, in una logica di continuità, uno statuto di garanzie alla sfera privata e inviolabile della persona.

Da siffatte osservazioni, emerge un concetto di domicilio "costituzionale" [371] tale da ricomprendere le nuove esigenze di tutela frutto del progresso tecnologico e altrettanto meritevoli di salvaguardia. In attesa di un puntuale intervento del legislatore in materia, devono ritenersi ammissibili limitazioni al c.d. "domicilio informatico" soltanto se conformi alla doppia regola della riserva di legge e di giurisdizione ai sensi dell'art. 14 Cost. Al pari dell'art. 15 Cost. anche siffatta disposizione prevede, infatti, un duplice meccanismo di tutela, per cui valgono le osservazioni prospettate poc'anzi, a cui si rinvia.

4. Il diritto alla riservatezza.

Fin qui, ci si è limitati ad analizzare le interferenze che la c.d *data retention* produce rispetto a due delle tradizionali libertà "negative"[372] di rango Costituzionale, la libertà di corrispondenza e la libertà di domicilio. Inoltre, nel delinearne i rispettivi sistemi di tutela, si è riscontrato che gli art. 14 e 15 Cost. sono ascrivibili ad una matrice comune coincidente con il pieno sviluppo della personalità e dignità umana. Seppur concettualmente distinti, le libertà fondamentali previste dagli artt. 14 e 15 Cost., rientrano infatti nel nucleo di salvaguardie predisposto dall'art. 2 Cost. ai sensi del quale la Repubblica italiana «riconosce e garantisce i diritti inviolabili dell'uomo»[373].

---

[369] Aderiscono a questa impostazione BARILE, CHELI, *Domicilio (libertà di)*, in *Enc. Dir*., vol. X, Milano, 1962, 860.

[370] Menziona gli effetti di "deterritorializzazione" e di dematerializzazione conseguenti all'uso delle tecnologie ed all'avvento della rete COSTANZO, *Il ruolo del fattore tecnologico e le trasformazioni del costituzionalismo*, in *Associazione Italiana dei Costituzionalisti, Costituzionalismo e globalizzazione. Atti del XXVII Convegno Annuale.* (Salerno 22-24 novembre 2012), Napoli, 2014, 43.

[371] L'espressione è di DOMENICALI, *Tutela della persona negli spazi virtuali: la strada del "domicilio informatico"*, in *www.federalismi.it*, 2018, 7, 15.

[372] Sul punto SILVESTRI, *L'individuazione dei diritti della persona*, in AA. VV. *Diritti della persona e nuove sfide del processo penale. Atti del XXXII convegno nazionale* (Salerno, 25-27 ottobre 2018), Milano, 2019, 23.

[373] Per completezza, si riporta l'art. 2 Cost. per intero:

Siffatta norma è stata qualificata una "fattispecie aperta"[374] a cui sono riconducibili tutti i valori che consentono il pieno manifestarsi della personalità dell'individuo, indipendentemente dal fatto che essi trovino espresso riconoscimento nel dettato costituzionale. In tal senso, l'articolo 2 Cost. è dotato di grande "forza maieutica"[375] nell'opera di individuazione di "nuovi diritti" che accordano forme di tutela innovative ridefinendo i principi già esistenti.

Tra i valori riconducibili all'alveo di tutela predisposto dalla norma sopracitata, rientra indubbiamente il diritto alla riservatezza, privo di espressa previsione nell'ordinamento italiano. L'individuazione e la determinazione del contenuto di tale concetto sono infatti da ascrivere alla giurisprudenza del Giudice delle leggi[376] e della Corte di Cassazione. In particolare, quest'ultima ha individuato il nucleo essenziale della riservatezza nel potere di escludere interferenze altrui dalla propria vita privata. Siffatta pretesa può essere esercitata non soltanto entro i confini del "tradizionale domicilio domestico" ma anche rispetto a tutte le vicende strettamente personali «il cui carattere intimo è dato dal fatto che esse si svolgono in un domicilio ideale, non materialmente legato ai tradizionali rifugi della persona umana (le mura domestiche o la corrispondenza)» [377].

Si è pervenuto così all'individuazione di una "nuova" libertà negativa, tradizionalmente intesa come l'interesse alla non divulgabilità o alla conoscibilità esclusiva delle notizie riguardanti la propria "sfera personale"[378]. Inoltre, si è attribuito

---

«La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale.»

[374] L'inquadramento dell'art. 2 Cost. come un "catalogo aperto o chiuso" è stato oggetto di un lungo dibattito dottrinale. *Ex multis*, rilevano che la norma sia dotata di un carattere espansivo in grado di generare nuovi ed inediti diritti fondamentali e altrettante nuove dimensioni di tutela degli stessi SILVESTRI, *L'individuazione dei diritti della persona*, 24; CAVALIERE, *Questioni attuali in tema di "nuovi diritti"*, in *www.dirittifondamentali*, 2015, 12. In senso opposto, il contributo più significativo è di BARBERA, *Commento all'art. 2 della Costituzione*, in *Commentario della Costituzione*, (a cura di) BRANCA, Bologna, 1997.

[375] L'espressione è BALDASSARRE, *Diritti inviolabili*, in *Diritti della persona e valori costituzionali*, Torino, 1997, 61.

[376] Si fa riferimento in particolar modo alla Corte cost., sent. 12 aprile 1973, n. 38, in *Giur. Cost.*, 1973, 362 e ss. In tale pronuncia, la Corte ha affermato che i diritti inviolabili dell'uomo, tra i quali rientrano la tutela della propria rispettabilità e della propria riservatezza, sono riconducibili all'alveo di tutela predisposto dall'art. 2. Siffatta norma viene dunque concepita come una clausola aperta.

[377] Cfr. Cass. Civ., sez. III, 27 maggio 1975, n. 2129, Esfandiari, in *Riv. It. Dir. internaz.* 1980, 293 e ss.

[378] Si tratta della nozione di riservatezza accolta dall'orientamento dottrinale prevalente. Sul punto si vedano BRICOLA, *Prospettive e limiti della tutela penale della riservatezza*, in *Riv. It. Dir. proc. Pen*.,

alla riservatezza un ambito di applicazione autonomo[379] rispetto ai diritti tutelati dagli artt. 14 e 15 Cost.

Sulla base di tale premesse, è evidente che l'attività di acquisizione dei dati di traffico telefonico e telematico produca un'interferenza anche con il diritto alla riservatezza[380], frutto dell'elaborazione giurisprudenziale e dottrinale. Infatti, la trasmissione dei dati "esterni" alle autorità inquirenti da parte dei fornitori dei servizi elettronici viola l'interesse alla conoscenza esclusiva delle informazioni riguardanti la sfera privata. La pretesa dell'utente di evitare la divulgazione di suddetti dati rientra nella tutela della riservatezza[381].

Siffatta interferenza non deve essere confusa con quella prodotta dalla c.d. *data retention* rispetto alla segretezza delle comunicazioni. Seppur innegabile la stretta connessione tra la tutela della riservatezza e siffatto diritto fondamentale, gli interessi individuali garantiti risultano concettualmente distinti[382]. Nel caso di specie, l'articolo 15 Cost. tutela la pretesa dell'utente di evitare l'altrui conoscenza del fatto-comunicazione e di tutte le informazioni "esterne" ad essa inerenti. La compressione di tale prerogativa personale si realizza fin dal momento in cui i dati di traffico sono archiviati dai fornitori di servizi elettronici. Già in questa fase, tutte le informazioni personali inerenti alle comunicazioni effettuate sono conoscibili a terzi. In conclusione, costituisce una deroga rispetto al diritto alla segretezza delle comunicazioni non solo l'attività di acquisizione dei dati per finalità processuali ma anche l'archiviazione degli stessi da parte dei *service providers*[383].

La riservatezza, in quanto espressione della volontà individuale di non rendere manifesto ciò che attiene alla propria dimensione privata, aggiunge un ulteriore tassello. Sulla base di tale assunto, non solo i dati di traffico non dovrebbe essere resi

---

1967, 1088; PISANI, *La tutela penale della riservatezza: aspetti processuali*, in *Riv. It. Dir. proc. Pen.*, 1967, 786.

[379] L'autonomia semantica della nozione di riservatezza è sottolineata da CAPRIOLI, *Colloqui riservati e prova penale*, Torino, 2000, 17.

[380] Così ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, *cit.*, 50.

[381] Cfr. MANTOVANI, *Diritto alla riservatezza e libera manifestazione del pensiero con riguardo alla pubblicità dei fatti criminosi*, in *Arch. Giur*., 1968, 61.

[382] Sul punto. Si veda GAITO, FURFARO, *Intercettazioni: esigenze di accertamento e garanzie della riservatezza*, in GAITO (a cura di), *I principi europei del processo penale*, Roma, 2016, 363 e ss. Gli Autori sottolineano che la riservatezza in quanto «espressione in atto della volontà impressa dal soggetto a non rendere manifesto ciò che pone in essere o gli accade» deve essere «concettualmente distinta dal segreto». Sulla base di tale premesse, affermano inoltre che il diritto alla segretezza «va tutelato in sé»

[383] Per la definizione di *service provider* si rimanda al Cap. I.

conoscibili a terzi, ma ancor di più dovrebbe esserne impedita la divulgazione da chi legittimamente li detiene. Nella c.d. *data retention*, il venire meno di tale pretesa si realizza nel momento in cui i tabulati telefonici e telematici vengono trasmessi all'autorità giudiziaria.

5. Il diritto al rispetto della «vita privata e familiare» ai sensi degli articoli 8 CEDU e 7 CDFUE.

Mentre il diritto alla riservatezza ha trovato autonomo radicamento nell'ordinamento italiano a seguito di una serie di approdi giurisprudenziali risalenti nel tempo, soltanto negli ultimi anni si è sentita l'esigenza di riconoscere alla *privacy*[384] una tutela generalizzata[385]. Su impulso di istanze sovranazionali[386], si è via via ritenuta inidonea a soddisfare le nuove esigenze individuali l'idea intimistica di «vita privata», intesa come libertà dalle ingerenze altrui nella propria vita individuale. La crescente esposizione pubblica della persona causata dall'utilizzo delle nuove tecnologie[387] ha infatti determinato la progressiva transizione da una accezione "statica" della riservatezza, legata ad un'arcaica "logica domenicale", ad una più "dinamica". Accanto alla dimensione negativa dello *ius escludendi alios*[388], si è andata via via definendo la tutela della libertà "positiva" del singolo di intessere rapporti sociali con altre persone.

Pertanto, alla salvaguardia della «riservatezza», limitata ai paradigmi costituzionali nazionali, si è affiancata la più ampia e generalizzata tutela della *privacy*[389]. Soggetta ad un'intensa dilatazione interpretativa, siffatta nozione ha

---

[384] Analizza la pluralità di significati riconducibili al concetto di *privacy* TIBERI, *Riservatezza e protezione dei dati personali*, *cit*., 349 e ss.

[385] Sul punto si veda BONETTI, *Riservatezza e processo penale*, Milano, 2003, 15. L'Autore inoltre fornisce uno scenario completo del rapporto tra la tutela della *privacy* e il processo penale.

[386] Sottolinea il verificarsi di interscambi e integrazioni reciproche tra l'ordinamento interno e quello sovranazionale, nell'ambito del quale hanno un ruolo fondamentale le Carte dei diritti fondamentali, ILLUMINATI*, Libertà e segretezza della comunicazione*, in AA. VV. *Diritti della persona e nuove sfide del processo penale. Atti del XXXII convegno nazionale* (Salerno, 25-27 ottobre 2018), Milano, 2019, 157. L'Autore ha ricondotto il fenomeno di interferenze reciproche tra normative multilivello al c.d. "porosità" degli ordinamenti.

[387] Sul punto si veda RODOTÀ, *Prefazione*, in (a cura di) PANETTA, *Libera circolazione e protezione dei dati personali*, Milano, 2006, p. VIII.

[388] Si veda *supra*, Cap II § 3.

[389] Il termine «privacy» ha origini risalenti nel tempo. L'espressione compare per la prima volta nel famoso saggio intitolato «The right to privacy» in cui *Samuel Warren* e *Louis Brandeis* elaboravano la primigenia idea di un «diritto alla sfera privata che non deve essere toccata dall'Autorità pubblica» (*right to be alone*). Sul punto v. WARREN, BRANDEIS, *The Right to Privacy, in Harvard Law Review*,

ampliato nel corso del tempo il suo perimetro applicativo[390], fino a ricomprendere tutti gli elementi della sfera personale sottoposti all'autodeterminazione del singolo[391]. In siffatto concetto "fluido"[392] rientrano il diritto al rispetto della propria vita privata e familiare nonché la libertà positiva di esercitare un controllo effettivo sui propri dati personali. Come si è anticipato, tali aspetti di tutela, che si aggiungono alla dimensione eminentemente negativa del concetto di riservatezza, non trovano espresso riferimento nella Costituzione italiana. Sono invece oggetto di pieno riconoscimento nell'ordinamento sovranazionale grazie ad un complesso sistema di garanzie accordate dalle Carte europee dei diritti fondamentali[393] e alla loro interpretazione fornita dalle Corti[394].

A livello sovranazionale[395], il nodo centrale del complesso sistema "multilivello"[396] di tutela alla *privacy* trova fondamento nell'articolo 8 della CEDU[397]

Vol IV, Boston, n. 5, 1890, 193. Siffatta prospettiva secondo cui è opportuno tutelare l'individuo dal controllo che le autorità pubbliche esercitano sui cittadini è stata approfondita nel corso di tutto il XX secolo da filosofi e da sociologi, tra i quali è opportuno menzionare *Foucault*. Per un approfondimento sul tema v. LUPÀRIA, MARAFIOTI, *Confessione, liturgie della verità e macchine sanzionatorie. Scritti raccolti in occasione del Seminario di studio sulle «Lezioni di Lovanio» di Michel Foucault*, Torino, 2015.

[390]L'espressione è di LUPÁRIA, Privacy*, diritti della persona e processo penale,* in *Riv. dir. proc.*, LXXIV (6), 2019, 1448.

[391] Sul "diritto di autodeterminazione informativa" si tornerà nel Cap. III.

[392] Definisce la *privacy* un concetto fluido in quanto in *«costante relazione tra mutamenti delle tecnologie delle informazioni»* RODOTÀ, *La* privacy *tra individuo e collettività,* in *Pol. dir.,* 1974, 3, 551. Sul punto si veda anche CISTERNA, *Cedu e diritto alla* privacy, in GAITO (a cura di), *I principi europei del processo penale*, Roma, 2016, 194. Secondo l'Autore la *privacy* rientra nella categoria dei diritti "liquidi" «ossia anamorfici o metamorfici in quanto privi di connotati durevoli e stabili».

[393] Cfr. LUPÀRIA, *Diritto alla* privacy, in AA. VV. *Diritti della persona e nuove sfide del processo penale. Atti del XXXII convegno nazionale* (Salerno, 25-27 ottobre 2018), Milano, 2019, 98.

[394] Come si vedrà meglio in seguito, si fa riferimento sia alla Corte di Giustizia sia alla Corte EDU.

[395] In tale sede, è opportuno ricordare che, in base all della Corte Costituzionale, le norme della Convenzione, così come interpretate dalla Corte di Strasburgo, costituiscono parametro interposto di costituzionalità della legislazione interna ai sensi dell'art. 117 Cost. La CEDU è inquadrabile come fonte sovranazionale di rango infra-costituzionale che, nella gerarchia delle fonti, si trova su un gradino inferiore alla Costituzione. Sul punto si vedano le c.d. sentenze "gemelle" della Corte Costituzionale n. 348 e 349/2007, consultabili *online* presso *www.cortecostituzionale.it*.

[396] Vedi quanto detto *supra*.

[397] La Convenzione per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali, solitamente abbreviato in CEDU, è un trattato internazionale volto a tutelare i diritti umani e le libertà fondamentali in Europa. È stata firmata nel 1950 dal Consiglio d'Europa, di cui sono parte 47 paesi, 28 dei quali sono membri dell'Unione europea (UE). La presente Convenzione ha istituito la Corte europea dei diritti dell'uomo (o Corte EDU) che provvede a fornire una tutela giurisdizionale alle persone soggette a violazioni dei diritti umani. Per un maggiore approfondimento sulla struttura e sulle più recenti prospettive della Corte si veda RUGGIERI, *Corte europea dei diritti dell'uomo e giudici nazionali, alla luce della più recente giurisprudenza costituzionale (tendenze e prospettive)* in *Osservatorio costituzionale,* 2018, fasc. 1, 20.

che garantisce il rispetto della vita privata e familiare dell'individuo[398]. Nel corso degli anni, la nozione di «sfera privata» è stata ridefinita e ampliata[399] dai giudici della Corte fino a ricomprendere qualsiasi spazio di interazione con il mondo esterno al fine di tutelare l'interesse dell'individuo «di intessere e sviluppare relazioni con i propri simili»[400].

Nella cornice convenzionale, la giurisprudenza sovranazionale ha infatti predisposto una duplice tutela del diritto in oggetto: da un lato si è impegnata a garantire l'integrità fisica e morale della persona, nella sua dimensione individualistica e privata, dall'altro ha preso in considerazione la vita del singolo nella sua dimensione sociale e della sua capacità di intrattenere relazioni con altri. In tale seconda accezione rientra anche il diritto al controllo dei propri dati personali.

In tal senso, valorizzando la *vis espansiva* della formulazione adottata dal legislatore europeo, i giudici di Strasburgo hanno adottato un'interpretazione evolutiva della disposizione in esame, includendo nell'ambito di applicazione della norma la tutela delle informazioni digitali relative alla propria persona (c.d. *data protection*)[401]. L'articolo 8 CEDU ha dunque rappresentato la base normativa di elaborazione del diritto di nuovo conio inerente alla dimensione pubblica del binomio vita privata-libertà[402].

---

[398] L'articolo 8 della CEDU, rubricato «Diritto al rispetto della vita privata e familiare», prevede che**:**
«1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.
2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui».

[399] I giudici della Corte affermano che il sintagma «vita privata» è una «nozione ampia non suscettibile di definizione esaustiva». Si veda sul punto Corte EDU, Grande Camera, 4 dicembre 2008, S. e Marper c. Regno Unito, § 66. Per visionare *online* il testo completo della pronuncia si consulti *www.hudoc.echr.coe.int.*

[400] Cfr. C. EDU, Sez. V, 4 maggio 2000, Rotaru c. Romania; negli stessi termini Id., Sez. V, 2 settembre 2010, Uzun c. Allemagne.

[401] Si occupa espressamente della protezione dei dati personali e diritto di controllo sulla loro circolazione la Convenzione di Strasburgo n.108/1981 «sulla protezione delle persone rispetto al trattamento automatizzato di dati personali». Pur avendo ratificato la Convenzione, l'Italia è rimasta priva di una normativa di recepimento fino al 1995. Soltanto mediante l'emanazione della legge 675/1995, di attuazione della direttiva comunitaria 95/46/CE, l'ordinamento italiano ha potuto adeguarsi ai contenuti previsti dalla Convenzione. Per un approfondimento sul punto si veda *infra*.

[402] Sull'ampia dimensione del diritto al rispetto della vita privata, TIBERI, *Riservatezza e protezione dei dati personali*, in CARTABIA (a cura di), *I diritti in azione*, Bologna, 2007, 361 e ss.

Ciò posto, il diritto al rispetto della vita privata non gode di tutela assoluta[403], ma può essere soggetto a compressioni e limitazioni da parte delle autorità di *law enforcement*[404] per il perseguimento di interessi collettivi stabiliti dalla legge secondo il principio di legalità convenzionale[405]. Ai sensi dell'articolo 8 CEDU, paragrafo 2, ingerenze nella sfera privata sono ammesse soltanto qualora trovino fondamento in una norma di diritto interno, che risulti accessibile, prevedibile e chiara per i destinatari della misura restrittiva predisposta.

Inoltre, è orientamento diffuso in giurisprudenza che i requisiti qualitativi anzidetti siano calibrati in base all'invasività dell'ingerenza che è in grado di cagionare l'attività prevista nella disciplina nazionale. Secondo la Corte, laddove la compressione alla riservatezza del singolo sia realizzata mediante misure sottratte, *ex se*, al controllo e alla conoscibilità delle persone interessate, il legislatore nazionale è tenuto ad indicare con precisione «in quali circostanze e a quali condizioni autorizza la pubblica autorità ad operare simile violazione segreta»[406]. Al contrario, ove la misura sia dotata di minore invasività, si ritiene sufficiente che la base legale sia precisa e non dia luogo a dubbi ermeneutici.[407]

In aggiunta alle condizioni suesposte, la norma richiede che l'intrusione da parte delle pubbliche autorità sia «necessaria» in una «società democratica» sulla base del legittimo scopo perseguito. Secondo la Corte di Strasburgo, non solo è necessario che la misura trovi legittimazione nell'interesse a salvaguardare il sistema istituzionale democratico, ma è altresì richiesto che sia «proporzionata rispetto alla giustificazione invocata»[408]. Il legislatore nazionale è, dunque, chiamato a valutare la proporzionalità

[403] Secondo un approccio analogo a quello adottato anche negli articoli 9-11 CEDU. Sono, invece, assolutamente inviolabili perché non soggetti ad alcuna deroga o limitazione i diritti individuati dall'art. 15, co. 2, CEDU.
[404] Con tale espressione si fa riferimento alle forze dell'ordine, all'Autorità giudiziaria e a tutti gli organi competenti al mantenimento dell'ordine pubblico.
[405] Sul punto, si veda ANDOLINA, *L'ammissibilità degli strumenti di captazione dei dati personali tra standard di tutela della* privacy *e onde eversive*, in *Arch. pen.*, 2015, n. 3, 920.
[406]Cfr. Corte EDU, 2 agosto 1984, Malone c. Regno Unito, § 66-68. Per consultare la versione integrale della sentenza si veda sempre *www.hudoc.echr.coe.int*.
[407]Cfr. Corte EDU, Sez. V, 2 settembre 2010, Uzun c. Allemagne, cit. Nel corso di siffatta pronuncia, i giudici affermano che i criteri più severi stabiliti e applicati nell'ambito della sorveglianza delle comunicazioni elettroniche non operano nei confronti di misure, come la localizzazione tramite GPS, che inferiscono con minore intensità nella sfera privata della persona.
[408]Sul punto si veda Corte EDU, Klass e altri c. Germania, *cit.* § 42.

della misura restrittiva prescelta con il fine pubblico legittimamente perseguito all'interno di un giudizio di proporzionalità[409].

Una volta delineati i caratteri essenziali dell'articolo 8 CEDU, è necessario verificare se nella tutela della «corrispondenza» possano essere ricomprese anche altre forme di comunicazione, tra cui quelle telefoniche e telematiche[410]. Ebbene, in riferimento a tali strumenti, è da segnalare un orientamento consolidato della Corte di Strasburgo[411] secondo cui le conversazioni telefoniche e telematiche rientrano nel raggio di applicazione dell'art. 8, par 1, CEDU. Ciò posto, il passaggio successivo consiste nel verificare se la c.d. *data retention* rappresenti *ex se* un'interferenza rispetto al diritto alla «vita privata» dell'individuo.

La questione è stata affrontata più di trenta anni fa dalla Corte EDU con la storica pronuncia sul caso *Malone*, durante il quale si è discussa la legittimità della conservazione dei dati di traffico delle comunicazioni elettroniche nel Regno Unito (c.d. *metering o comptage*[412]). Dopo aver specificato che «i numeri chiamati costituiscono un elemento integrante della comunicazione telefonica», ha osservato che l'acquisizione di queste informazioni da parte degli organi inquirenti rappresenta un'interferenza rispetto al diritto garantito dall'articolo 8 CEDU[413]. Di conseguenza, i giudici della Corte di Strasburgo hanno affermato che la portata dell'articolo in oggetto ricomprende tutte le attività di raccolta, archiviazione e apprensione dei dati di traffico realizzate senza il consenso dell'interessato. L'attività di *metering* risulta, dunque, ammissibile soltanto qualora rientri nei casi previsti dalla legislazione nazionale per il perseguimento di un interesse pubblico all'interno di una società democratica.

Tale assunto è stato più volte ribadito in procedimenti più recenti in cui la Corte ha avuto modo di confermare che la schedatura e la registrazione in banche dati gestiti

---

[409] In seguito, si vedrà approfonditamente come analoghe condizioni di legittimità sono richiamate, nell'ambito dell'ordinamento UE, in merito alla tutela della riservatezza e al diritto alla protezione die dati di carattere personale ai sensi degli articoli 7 e 8 CDFUE. Sul punto, si rimanda a quanto affermato dalla CGUE nella sentenza *Digital Rights Ireland* in Cap II § 8.

[410] ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, *cit.*, 41.

[411] Cfr. Corte EDU, Klass e altri c. Germania, *cit.* § 41; Corte EDU, sent. 1° luglio 2008, Liberty e altri c. Regno Unito, § 56.

[412] Con tale espressione si fa riferimento all'attività di registrazione e conservazione automatica dei dati esteriori delle conversazioni. L'operazione rientra dunque nella nozione di *data retention*.

[413] Cfr. Corte EDU, 2 agosto 1984, Malone c. Regno Unito, § 69.

da organi pubblici o privati sono in grado di realizzare compromissioni indebite nella vita privata altrui[414].

Le medesime osservazioni possono farsi in merito all'art. 7[415] della Carta di Nizza, dedicato al «rispetto[416] della vita privata e familiare», la cui *ratio* è chiaramente ispirata al contenuto dall'art. 8 CEDU[417]. Inoltre, sulla base di quanto stabilito dall'art. 52, par. 3, CDFUE[418], il significato e la portata dei diritti previsti dall'art. 7 sono esattamente «identici»[419] a quelli garantiti dal corrispondente articolo della Convenzione europea. Da siffatta precisazione, contenuta nelle "Spiegazioni relative alla Carta"[420], deriva che «le limitazioni che vi possono legittimamente essere apportate sono pertanto quelle autorizzate ai sensi del suddetto articolo 8»[421]. Pertanto, le legislazioni nazionali possono prevedere deroghe alla tutela della vita privata dell'individuo soltanto mediante misure ritenute «necessarie» all'interno di una «società democratica»[422].

Ciò posto, è opportuno rimarcare un'interessante differenza tra i due articoli[423]. Il termine «corrispondenza», contenuto nell'articolo 8 della CEDU, è stato sostituto

---

[414]Cfr. Corte EDU, Grande Camera, 16 febbraio 2000, Amann c. Svizzera, in *Dir. pen. proc.*, 2000, 645.
[415] L'art. 7 CDFUE dispone che «Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni».
[416] Come ha sottolineato la dottrina, il termine «rispetto» sembra dare una connotazione soprattutto negativa al diritto alla vita privata. Sul punto si veda GROPPI, *sub* art. 7*,* in *L'Europa dei diritti, commento alla Carta dei diritti fondamentali dell'Unione Europea*, BOLOGNA, BIFULCO, CARTABIA, CELOTTO, (a cura di), 2001, 76 e ss.
[417] Sul punto si veda MARTINICO, *Commento all'art. 7 della Carta*, in MASTROIANNI, POLLICINO, ALLEGREZZA, PAPPALARDO, RAZZOLINI, *Carta dei diritti fondamentali dell'Unione europea*, Milano 2017, 116.
[418]L'art. 52, par 3, della Carta di Nizza dispone che «Laddove la presente Carta contenga diritti corrispondenti a quelli garantiti dalla Convenzione europea per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali, il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta convenzione. La presente disposizione non preclude che il diritto dell'Unione conceda una protezione più estesa».
[419] Così si sono espresse le "Spiegazioni relative alla Carta". Si veda *nota 420*.
[420] Si tratta di spiegazioni elaborate sotto l'autorità del *praesidium* della Convenzione che ha redatto la Carta dei diritti fondamentali dell'Unione europea. Più di recente, sono state aggiornate in base agli adeguamenti redazionali che siffatta Convenzione ha apportato al testo della Carta. Sebbene non abbiano efficacia legislativa, rappresentano un importante strumento per chiarire l'esegesi delle disposizioni della Carta. Sono state pubblicate nella Gazzetta ufficiale dell'Unione europea il 14 dicembre 2007. Per consultare il testo *online* si veda *www.fra.europa.eu.* Per un approfondimento sulla "natura" delle Spiegazioni si veda invece SCIARABBA, *Le "spiegazioni" della Carta dei diritti fondamentali dell'Unione*, DPCE, 2005, 59 e ss.
[421] Nel senso, però, che la Carta di Nizza può assicurare una tutela anche più estesa di quella prevista dalla CEDU si veda GROPPI, *sub* art. 7*,* in *L'Europa dei diritti, commento alla Carta dei diritti fondamentali dell'Unione Europea*, *cit*., 80.
[422] Si rimanda a quanto detto *supra* in merito all'art. 8 della CEDU.
[423] Per un approfondimento sulle ulteriori differenze che esistono tra l'art. 7 CDFUE e l'art. 8 della CEDU si veda MARTINICO, *Commento all'art. 7 della Carta*, in MASTROIANNI, *OP. cit.*, 116 e ss

con la più moderna espressione «comunicazioni» per – come sottolineano le Spiegazioni – «tener conto dell'evoluzione tecnica». Questo cambiamento di linguaggio elimina ogni dubbio sulla portata applicativa dell'articolo in esame che, dunque, predispone la tutela di ogni forma di comunicazione con qualsiasi strumento essa sia effettuata.

Una volta chiarito il contenuto essenziale dell'art. 7 CDFUE, per l'analisi delle interferenze che la c.d. *data retention* produce nei confronti dei diritti da esso tutelati, si rimanda a quanto affermato dalla Corte di Giustizia nel caso *Digital rights Ireland*[424].

6. Il diritto alla protezione dei dati di carattere personale.

Come si è anticipato, l'ulteriore traguardo evolutivo in materia di *privacy*[425] si è raggiunto mediante la configurazione della c.d. *data protection* quale autonomo diritto fondamentale della persona[426]. La libertà dell'individuo di esercitare un controllo effettivo sul flusso dei propri dati personali[427] non è prevista nella Costituzione italiana, né nella Convenzione europea dei diritti dell'uomo[428]. È, infatti, in ambito comunitario che si perfeziona la messa a fuoco di questo nuovo paradigma normativo attinente alla «dimensione esterna» della riservatezza[429].

---

[424] La pronuncia della Corte di Lussemburgo verrà approfondita ampiamente *infra*.

[425] L'art. 8 CDFUE rappresenta la "sublimazione" dell'approdo del diritto alla *privacy,* da una dimensione prevalentemente negativa, legata all'elaborazione originaria di Warren e Brandeis (sul punto si veda *supra*) ad una di carattere positivo. In tal senso, BASSINI, POLLICINO, *Commento all'art. 8 della Carta*, in MASTROIANNI, POLLICINO, ALLEGREZZA, PAPPALARDO, RAZZOLINI, *Carta dei diritti fondamentali dell'Unione europea*, Milano 2017, 136.

[426] Sul punto si veda LUPÀRIA, *Privacy, diritti della persona e processo penale, cit.*, 1452. L'Autore sottolinea che dal tradizionale concetto di *privacy* sia avvenuta una «gemmazione di diritti» volta ad ampliare la tutela della sfera personale. A seguito di tale fenomeno di "proliferazione normativa", la tradizionale libertà negativa di non subire interferenze nella propria vita privata risulta affiancata da una serie di libertà positive che aggiungono nuove prospettive di tutela.

[427] Ai sensi dell'art. 4 del GDPR, si definisce dato personale «qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale». Sul punto, si vedano anche i Considerando 26, 27 e 30 del GDPR.

[428]Eppure, a riprova del contenuto flessibile della Convenzione, è possibile rinvenire molteplici pronunce della Corte di Strasburgo in materia di *data protection*, a cui spesso si fa riferimento come «informational privacy». Per un quadro aggiornato si veda Consiglio d'Europa, *Guide on Article 8 of the European Convention on Human Rights*, 38 e ss. *su www.echr.coe.int*.

[429] Cfr. LUPÁRIA, Privacy*, diritti della persona e processo penale,* in *Rivista di diritto processuale*, LXXIV (6), 2019, 1452.

All'interno dei Trattati dell'Ue, viene in rilievo l'art. 16 TFUE[430] che, in combinato disposto con l'art. 39 TUE[431], attribuisce alle istituzioni europee una competenza specifica in materia di protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale[432]. Si raggiunge, però, il punto di approdo del processo di "costituzionalizzazione" della c.d. *data protection,* mediante la codificazione dell'art. 8 CDFUE[433] che assegna autonoma rilevanza giuridica al diritto alla protezione dei dati, accanto al più tradizionale diritto al rispetto della vita privata[434]. La cristallizzazione di tale "nuovo"[435] diritto all'interno della Carta di Nizza è frutto di un contesto sociale radicalmente mutato rispetto a quello in cui era nata la CEDU e più sensibile alle esigenze insorte a seguito della "Rivoluzione informatica"[436].

Una volta enunciato il principio cardine secondo cui si garantisce a ciascun individuo la protezione dei propri dati personali, la disposizione sopracitata disciplina specifici requisiti in base ai quali è possibile che gli stessi siano sottoposti ad un

---

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

[431] L'art 39 del TUE prevede che «Conformemente all'articolo 16 del trattato sul funzionamento dell'Unione europea e in deroga al paragrafo 2 di detto articolo, il Consiglio adotta una decisione che stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del presente capo, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti».

[432] Sul punto si veda CORTESE, *La protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona*, in *Il dir. dell'Ue*, 2013, 315.

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

[434] Sul punto si rimanda a quanto detto *supra*.

[435] In realtà, non si tratta propriamente di un "nuovo" diritto in quanto la Carta di Nizza si è limitata a consolidare quanto già affermato dalla giurisprudenza delle Corti internazionali e nazionali. In particolar modo, mediante il diritto alla tutela dei dati personali codificato dall'art. 8 della CDFUE si è apprestata una tutela più estesa alla «Informationelle Selbstbestimmung» (diritto all'autodeterminazione informativa) creata a partire dagli anni Ottanta dalla Corte Costituzionale tedesca. Sul punto si veda BASSINI, POLLICINO, *Commento all'art. 8 della Carta*, *cit.*, 136.

[436] Cfr. *Introduzione*.

«trattamento»[437] da parte di terzi. In primo luogo, è necessario che l'interessato abbia prestato il proprio «consenso»[438] oppure che sussista un altro «fondamento» previsto dalla legge nazionale. Inoltre, l'operazione a cui sono sottoposti i dati deve ritenersi necessaria (art 8, par. 2, CDFUE) e subordinata al controllo di un'autorità indipendente (art 8, par. 3, CFDUE). In sintesi, la *ratio* della norma in esame consiste nell'attribuire all'individuo il pieno controllo di tutte le informazioni che divulgano elementi essenziali della propria vita privata e nel limitare le ingerenze da parte di terzi allo stretto necessario.

Per capire con quali strumenti il legislatore comunitario abbia inteso garantire, nel corso del tempo, la tutela del diritto in esame, è necessario fare riferimento al quadro normativo in materia di protezione dei dati personali nell'ordinamento UE[439].

In primis, è opportuno menzionare la Convenzione di Strasburgo n. 108/1981[440] che, mediante l'introduzione dei principi alla base di un trattamento legittimo (liceità, pertinenza rispetto alla finalità perseguita, qualità dei dati *etc. etc.*)[441], ha rappresentato la spinta propulsiva per la formazione di un *corpus* normativo autonomo in materia. Siffatte istanze sono state poi recepite dalla direttiva

[437] È definito «trattamento» ai sensi dell'art 4, n. 2, del GDPR «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione».

[438] Dicasi «consenso dell'interessato» ai sensi dell'art. 4, n. 11, del GDPR «qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento». Sul punto si vedano anche i Considerando 32 e 33.

[439] Sul punto si veda CORTESE, *La protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona*, in *Il dir. dell'Ue*, 2013, 320.

[440] Siffatto strumento normativo, già citato nella presente ricerca, rappresenta uno degli strumenti legali più importanti predisposti alla tutela del trattamento automatizzato dei dati personali. Per quanto riguarda il procedimento di ratifica della Convenzione da parte del legislatore italiano si rimanda alla nota 124.

[441] In breve, la Convenzione predispone che i dati possono essere raccolti e trattati solo in base a disposizioni interne che autorizzino il trattamento per specifiche finalità a cui devono essere destinati (art. 4). Inoltre, vieta la conservazione dei suddetti oltre il tempo necessario per raggiungere lo scopo prefissato (art. 5) e stabilisce il diritto dell'interessato ad ottenere informazioni in merito alla conservazione dei propri dati (art. 8). Come osservato *supra*, si tratta dei principi fondamentali alla base della normativa attuale in materia di protezione dei dati personali. Per consultare *on line* il testo della direttiva si veda *www.rm.coe.int.*

95/46/CE[442], c.d. direttiva "madre", relativa alla «tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati».

Mediante tale atto, il legislatore europeo ha coniugato il valore della *data protection* con il principio della libera circolazione dei dati per garantire la piena attuazione del «mercato interno» tra gli Stati membri anche in ambito digitale[443]. In sintesi, la direttiva ha recepito il contenuto della Convenzione estendendolo a qualsiasi «trattamento di dati», anche automatizzato[444]. Tra le novità da essa introdotte, figuravano la subordinazione del trattamento dei dati al consenso dell'interessato (libero e informato)[445], il riconoscimento in capo allo stesso del diritto di accesso ai dati conservati[446] e il diritto di opposizione[447]. Inoltre, l'atto sopracitato stabiliva che chiunque potesse disporre di un ricorso giurisdizionale in caso di violazione delle disposizioni nazionali applicabili al trattamento subito[448].

Siffatto apparato di garanzie era, però, oggetto di continue erosioni da parte di un diritto derivato sempre più incline a privilegiare esigenze di sicurezza nazionale[449] a discapito della tutela della vita privata nel settore delle comunicazioni elettroniche. Tale tendenza ha trovato ampio riscontro nell'emanazione della "storica" direttiva 2006/24/CE[450]. Con l'obiettivo di armonizzare le normative degli Stati membri aventi ad oggetto la conservazione dei dati di traffico per il perseguimento di gravi reati, la direttiva c.d. Frattini introduceva un obbligo sistematico e generalizzato di *data storage* in capo ai fornitori dei servizi di comunicazione elettronica (art. 3). Inoltre,

---

[442] Si tratta della «Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995. Tale atto legislativo è stato abrogato il 27 aprile 2016 con l'entrata in vigore del Regolamento 2016/679. Mediante l'emanazione del GDPR si è assistito ad un ribaltamento di prospettiva passando da un sistema incentrato sulle prerogative dell'interessato, tipico della direttiva 95/46/CE, ad uno basato sulla responsabilità del titolare della società di comunicazioni. sul punto si veda PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, 153 ss.

[443] In tal senso, si veda il Considerando 5 della Direttiva 95/46/CE.

[444] Cfr. Considerando 11 e 27.

[445] Cfr. Art. 2 lett. *h)* in cui la Direttiva forniva una definizione di «consenso della persona interessata».

[446] Cfr. Art. 12 della direttiva 95/46/CE.

[447] Cfr. Art. 14 della direttiva 95/46/CE.

[448] Cfr. Art. 22 della direttiva 95/46/CE.

[449] Ciò soprattutto a causa della crescente minaccia rappresentata dal dilagante fenomeno del terrorismo internazionale. Sul punto, si veda ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, *cit.*, 67.

[450] Si fa riferimento alla direttiva del Parlamento europeo e del Consiglio del 15 marzo 2006 «riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione». Tra gli studiosi lo strumento è conosciuto anche come "direttiva Frattini".

prevedeva che siffatta attività di archiviazione dei dati "esterni" alla conversazione potesse essere protratta «per periodi non inferiori a sei mesi e non superiori a due anni dalla data della comunicazione»[451].

Nell'impianto normativo predisposto dalla direttiva 2006/24/CE, il diritto alla protezione dei dati personali ex art. 8 CDFUE, *sub specie* dei "dati di traffico", veniva compromesso quasi del tutto a discapito di esigenze investigative e processuali. Tramite l'analisi della declaratoria di inefficacia della direttiva 2006/24/CE da parte della Corte di Lussemburgo e dell'*iter* argomentativo dei giudici, si avrà modo di approfondire il contenuto dell'atto di diritto derivato e le criticità in esso sussistenti. Inoltre, si acquisiranno maggiori strumenti per capire in che modo l'istituto della *data retention* entri in contrasto con i diritti di rango sovranazionale summenzionati.

7. *Data retention versus Data protection*: il percorso "travagliato" della direttiva 2006/24/CE.

Come si è accennato in precedenza[452], l'approvazione della direttiva 2006/24/CE è stata oggetto di ampio dibattito in ambito europeo[453] e, fin dalla sua entrata in vigore, sono stati sollevati dubbi di legittimità in merito al suo contenuto[454].

Già il Gruppo di lavoro "Articolo 29"[455], un organo europeo indipendente formato dalle autorità nazionali di protezione dei dati, aveva espresso non pochi dubbi circa le disposizioni della direttiva sopracitata. In particolare, con parere n. 3/2006[456], aveva affermato che la decisione di conservare per due anni tutti i dati di traffico dei cittadini europei avrebbe avuto un grande impatto sulla loro *privacy.* Al fine di limitare

[451] Cfr. art 6 della direttiva 2006/24/CE.
[452] Cfr. Cap I § 3.5.
[453] In tal senso, MARCOCCIO, Data retention*, la "Pisanu" dovrà fare i conti con l'Europa*, 2007, in *www.interlex.it*. EAD., Data retention, *cosa prevede la direttiva europea*, *IBIDEM.*
[454] In realtà anche prima della sua entrata in vigore vi è stato un ampio dibattito circa il contenuto della direttiva. Mediante il parere 4/2005 (v. doc. 113/2005) sulla proposta di direttiva presentata dalla Commissione europea (Com (2005) 438), il Garante europeo della protezione dei dati (GEPD) aveva espresso serie perplessità in merito ad una conservazione automatica e generalizzata di dati di traffico. In quanto incidente sul diritto fondamentale della riservatezza delle comunicazioni, questi riteneva che l'adozione di tale misura potesse essere legittima soltanto in casi eccezionali.
[455] Il Gruppo di lavoro "Articolo 29" (Art. 29 WP) era un organo consuntivo europeo che, fino al 25 maggio del 2018 (entrata in vigore del GDPR) si occupava di questioni relative alla protezione della vita privata e dei dati personali. Era composto da un rappresentante delle autorità nazionali di vigilanza e protezione dei dati di ciascuno Stato membro, dal Garante europeo della protezione dei dati e da un rappresentante della Commissione Ue. Gli archivi riguardanti l'attività dell'Art. 29 WP sono consultabili sul sito *www.edpb.europa.eu.*
[456] È possibile consultare *online* il parere sopracitato su *www.garanteprivacy.it*

l'incidenza sui valori e le libertà fondamentali dell'individuo, il Gruppo ribadiva la necessità di fornire, in fase di attuazione, indicazioni chiare e precise in merito alla finalità della conservazione. Inoltre, si riteneva necessario che gli Stati membri limitassero l'accesso ad una categoria di dati ristretta.

Dopo la sua entrata in vigore, la direttiva è stata oggetto di un ricorso di annullamento dinanzi alla Corte di giustizia da parte dell'Irlanda[457]. La ricorrente contestava la base giuridica dell'atto[458], ritenendo non corretto il richiamo all'art 95 del Trattato CE. Si sosteneva, infatti, che il «centro di gravità» della normativa in materia di *data retention* non fosse il funzionamento del mercato interno, ma la lotta al crimine che trovava legittimazione giuridica nel titolo VI del Trattato UE allora in vigore[459]. Il ricorso non è stato però accolto dalla Corte di Lussemburgo, la quale ha ritenuto che il legislatore europeo avesse fondato correttamente l'atto in esame sul primo e non sul terzo pilastro[460]. Nella sentenza, però, i giudici specificavano che «l'azione proposta dall'Irlanda riguardava solo la scelta del fondamento normativo e non una possibile violazione dei diritti fondamentali, scaturente dall'interferenza con il diritto alla *privacy* contenuta nella Direttiva 2006/24»[461].

7.1 Il dibattito presso le Corti costituzionali degli Stati membri (cenni).

Negli anni successivi, la disamina giurisprudenziale si è concentrata presso le Corti costituzionali di alcuni paesi membri che hanno censurato di volta in volta alcune

[457] Si veda Corte giust. UE, Grande Sezione, 10 febbraio 2009, *Irlanda c. Parlamento europeo*, causa C-301/06, in *www.curia.europa.eu* ed il commento di FABBRINI, *Lotta al terrorismo e tutela dei dati personali alla luce della sentenza Irlanda c. Parlamento e Consiglio*, in *Quaderni Costituzionali*, 2009, 419 ss.

[458] Sottolinea come la causa de qua sia un esempio della conflittualità tipica nell'assetto antecedente all'entrata in vigore del Trattato di Lisbona caratterizzato dalla «guerra tra pilastri» TIBERI*, La Corte di giustizia sulla conservazione dei dati: la protezione dei diritti fondamentali nel «dopo-Lisbona»,* in Quad. Cost., 2014, 722.

[459] Si fa riferimento alla versione del TUE antecedente alle modifiche apportate dal trattato di Lisbona. In particolare, vengono richiamati nella sentenza gli artt. 30 UE 31, n. 1, lett. c), UE, e 34, n. 2, lett. b), UE.

[460] Si fa riferimento alla suddivisione nei tre pilastri dell'Unione Europea, istituiti con il Trattato di Maastricht del 1992 e successivamente aboliti con l'entrata in vigore del Trattato di Lisbona nel 2009. In base a tale ripartizione, il primo pilastro riguardava le Comunità europee (CE), e cioè il mercato comune europeo e l'unione economica e monetaria. Il secondo era relativo alla Politica estera e di sicurezza (PESC); il terzo alla cooperazione nei settori della giustizia e degli affari interni (GAI).

[461] Paragrafo 57 della sentenza sopracitata.

disposizioni di recepimento della normativa europea[462]. Tutte le decisioni sono caratterizzate da una linea argomentativa comune perché basata sul giudizio di bilanciamento tra esigenze investigative e tutela della vita privata degli utenti sottoposti a conservazione dei dati.

Mediante tali pronunce, i tribunali nazionali hanno contribuito all'individuazione di *standard* processuali e sostanziali in tema di *data retention,* ponendo le fondamenta di quanto poi enunciato nella storica sentenza *Digital Rights Ireland Ltd e Seitlingler*. Si è, inoltre, assistito alla condivisione di valori e principi in tema di diritti fondamentali che hanno portato alla individuazione di uno *ius commune europeum*[463]. Per le ragioni appena enucleate, seguirà un richiamo alle pronunce più rilevanti.

La prima decisione in ordine cronologico è stata emessa dal Supremo Tribunale bulgaro[464] che ha dichiarato incostituzionale la norma nazionale di attuazione della direttiva 2006/24/CE. Nella sentenza, si sottolineava l'illegittimità di un meccanismo di conservazione automatica dei dati di traffico predisposto senza il controllo dell'autorità giurisdizionale. Inoltre, veniva per la prima volta approfondito il rapporto tra l'attività di *data storage* e il diritto al rispetto della vita privata tutelato dall'art. 8 della CEDU. Non si faceva invece alcun riferimento esplicito né alla Carta di Nizza né alla direttiva sopracitata[465].

In secondo luogo, è da ricordare la sentenza della Corte costituzionale della Romania del 8 ottobre 2009 che ha dichiarato l'illegittimità della legge n. 298/2008. Tale atto legislativo interno riconosceva in capo ai fornitori di servizi di comunicazione elettronica l'obbligo di archiviare i dati su semplice richiesta dell'autorità competente. Nel dichiarare l'incompatibilità tra tale previsione e l'art. 8, comma 2, della CEDU e l'art. 53 della Costituzione rumena, i giudici sottolineavano che a violare il diritto alla *privacy* non fosse il trattamento dei dati in sé ma il fatto che

---

[462] Cfr. GUELLA, Data retention *e circolazione dei livelli di tutela dei diritti in Europa: dai giudizi di costituzionalità rivolti alla disciplina UE al giudizio della Corte di giustizia rivolto alle discipline nazionali,* in DPCE *online*, 2017, 2.

[463] L'espressione è di TIBERI*, La Corte di giustizia sulla conservazione dei dati: la protezione dei diritti fondamentali nel «dopo-Lisbona*, *cit.*, 722.

[464] Si fa riferimento alla decisione dell'11 dicembre 2008, n. 13627, sez III che ha dichiarato l'incostituzionalità dell'art. 5 reg. 7.1.2000.

[465] CASCIONE*, I diritti fondamentali prevalgono sull'interesse alla sicurezza: la decisione* data retention *della Corte di Giustizia e gli echi del* datagate, in *Nuova Giur. Comm*., 2014, 11039.

fosse esteso indistintamente a tutti gli utenti. Il *puctum dolens* della disciplina interna consisteva, dunque, nel conferimento alle autorità inquirenti del potere di accedere ai dati di traffico di tutti i cittadini nazionali per motivi di «sicurezza nazionale»[466]. Non solo la norma non era connotata dal punto di vista soggettivo ma la finalità suindicata, non corredata da indicazioni più specifiche, non contribuiva a delimitarne l'angolo di applicazione.

Nello stesso senso si è espresso il Tribunale Costituzionale federale tedesco con sentenza resa nel marzo 2010[467]. Affrontando la legittimità costituzionale delle disposizioni in materia[468] di *Online Durchsuchung*[469] e *Vorratsdatenspeicherung* (c.d. *data retention*)[470], il *Bundesverfassungsgericht* è pervenuto a conclusioni di grande rilevanza anche a livello internazionale. Ha, infatti, contribuito ad individuare una serie di garanzie fondamentali che devono essere preservate nell'utilizzo di nuovi mezzi tecnologici di ricerca della prova, tra i quali rientra l'istituto della c.d. *data retention*.

Partendo dall'assunto che la tutela della segretezza delle comunicazioni non riguarda soltanto il contenuto della conversazione, ma anche le circostanze spaziali e temporali in cui questa si realizza, i giudici nazionali hanno affermato che l'istituto in esame debba essere inquadrato come una misura eccezionale. Inoltre, per evitare che nei cittadini si ingeneri la sensazione dell'istaurazione di un regime di *mass surveillance* da parte degli organi di polizia e dello Stato[471], si è ritenuto che l'istituto in esame debba rispondere al principio di proporzionalità. La normativa nazionale deve, dunque, contenere precise indicazioni circa i casi in cui si possa disporre la

---

[466] Sul punto si veda FLOR, *Data retention e limiti al potere coercitivo dello stato in materia penale: le sentenze del* Bundesverfassungsgericht *e della* Curtea Constitutionala, in *Cass. pen*., 2011, 1960.
[467] Si fa riferimento alla sentenza del 2 marzo 2010 *Bundesverfassungsgericht, sez III (1BvR 256/08).* Per consultare il testo della sentenza in lingua inglese si *veda www.bundesverfassungsgericht.de.* La sentenza è commentata da DI MARTINO*, Il* Bundesverfassungsgericht *dichiara l'incostituzionalità della* data retention *e torna sul rapporto tra libertà e sicurezza*, in *Giur. Cost.,* 2010, 4059 ss.
[468] Venivano richiamati gli articoli 113a e 113b *Telekommunikationsgesetzes* che risultavano in contrasto con gli articoli 1, 2 e 10 della *Grundsetz*, la Costituzione tedesca.
[469] *Online Durchsuchung* può essere tradotta in inglese con il termine *online search* o *online surveillance*. Mediante tale attività di indagine si realizza un monitoraggio prolungato di un sistema informatico *online*. Per un maggior approfondimento sul punto si veda FLOR, *Investigazioni ad alto contenuto tecnologico e tutela dei diritti. Fondamentali della persona nella recente giurisprudenza del* Bundesverfassungsgericht*: la decisione del 27 febbraio 2008 sulla* Online Durchsuchung *e la sua portata alla luce della sentenza del 2.3.2010 sul* data retention*,* in *Ciberspazio e dir.*, 2010, 365 (*note* 9 e 10).
[470] Si tratta dell'attività di accesso ai tabulati telefonici che viene svolta da un organismo di intelligence a "protezione della Costituzione", il *Verfassungsschutzbehörde*.
[471] FLOR, *Investigazioni ad alto contenuto tecnologico e tutela dei diritti. Fondamentali della persona nella recente giurisprudenza del* Bundesverfassungsgericht*, cit., 367.*

conservazione dei dati, le condizioni preliminari a cui subordinarne l'accesso e ulteriori precisazioni che ne garantiscano l'integrità probatoria.

7.2 La "valutazione d'impatto" della Commissione europea.

Davanti a tali pronunce delle Corti costituzionali europee, la Commissione europea ha presentato dinanzi al Consiglio ed al Parlamento europeo una relazione recante la "Valutazione dell'applicazione della direttiva sulla conservazione dei dati (direttiva 2006/24)"[472]. L'analisi della Commissione si basava sulle discussioni approfondite condotte con gli Stati membri[473] e le comunicazioni relative all'attuazione dell'atto europeo trasmesse da ventidue Stati membri[474].

In primo luogo, il rapporto evidenziava che l'articolo 15, paragrafo 1[475], della direttiva in esame aveva lasciato agli Stati membri un margine di manovra così ampio da renderne problematica la "valutazione di impatto"[476]. Sussistevano – e tuttora permangono – consistenti divergenze tra le legislazioni nazionali in merito alla finalità di accesso ai dati, ai periodi di conservazione e ai sistemi di sicurezza adottati dai gestori dei servizi di comunicazione elettronica. Inoltre, si rimarcava che alcuni Stati membri non avessero provveduto affatto al recepimento dell'atto di diritto derivato.In

---

[472] Si fa riferimento alla Relazione della Commissione europea del 18 aprile 2011. Per visionare il testo in versione integrale si veda COM (2011) 225 definitivo su *www.eur-lex.europa.eu.*

[473] Nel maggio 2009 la Commissione europea ha tenuto una conferenza intitolata «Towards the Evaluation of the Data Retention Directive», alla quale hanno preso parte le Autorità nazionali di protezione dei dati, enti privati interessati e gli accademici di diversi Stati membri. Sulla base di quanto discusso, la Commissione ha elaborato e inviato a tali parti interessate un questionario ricevendo più di settanta risposte. In seguito, si è organizzata una seconda conferenza nel dicembre 2010, intitolata «Taking on the Data Retention Directive», alla quale ha partecipato un gruppo analogo di studiosi e operatori del settore, per scambiare valutazioni preliminari della direttiva e discutere le sfide future in materia di *data retention*.

[474] Tra i ventidue Stati rientrano il Belgio, la Bulgaria, la Danimarca, l'Estonia, l'Irlanda, la Grecia, la Spagna, la Francia, l'Italia, Cipro, la Lettonia, la Lituania, il Lussemburgo, l'Ungheria, Malta, i Paesi Bassi, la Polonia, il Portogallo, la Slovenia, la Slovacchia, la Finlandia e il Regno Unito). Non si erano adoperati nel recepimento della direttiva la Repubblica Ceca, dalla Germania, dall'Austria, dalla Romania e la Svezia. Si veda la Tabella 1 della COM (2011) 225 (*nota 17*).

[475] L'art. 15, paragrafo 1, della direttiva 2006/24/CE, prevedeva che «Gli Stati membri mettono in vigore le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla presente direttiva al più tardi entro il 15 settembre 2007. Essi comunicano immediatamente alla Commissione il testo di tali disposizioni».

[476] In tal senso il Considerando 6 della Direttiva sopracitata dispone che «Le differenze giuridiche e tecniche fra le disposizioni nazionali relative alla conservazione dei dati ai fini di prevenzione, indagine, accertamento e perseguimento dei reati costituiscono un ostacolo al mercato interno delle comunicazioni elettroniche, giacché i fornitori dei servizi devono rispettare esigenze diverse per quanto riguarda i tipi di dati relativi al traffico e i tipi di dati relativi all'ubicazione da conservare e le condizioni e la durata di tale conservazione».

conclusione, l'emanazione della direttiva, aveva dato luogo ad un'armonizzazione della disciplina soltanto parziale, che precludeva un approccio comune[477] sull'intera materia della *data retention*.

In secondo luogo, si rilevava che la direttiva aveva imposto agli Stati membri di provvedere alla conservazione dei dati, non assicurandosi che tale attività avvenisse nel rispetto dei diritti fondamentali dell'individuo. L'atto legislativo trascurava quasi del tutto le fasi di immagazzinamento e di estrazione dei dati realizzate dai gestori dei servizi. In tal modo non veniva garantita l'integrità e la sicurezza dei dati per tutto il periodo di archiviazione presso i gestori dei servizi.

Da ultimo, la Commissione affermava l'importanza che agli operatori, soprattutto quelli di piccole dimensioni, fosse rimborsato il costo considerevole sostenuto per l'archiviazione dei dati.

Sulla base delle evidenze prospettate e del parere del Garante europeo per la protezione dei dati personali[478], la Commissione sottolineava la necessità di norme più precise e rispettose della vita privata e della riservatezza delle comunicazioni. In un momento storico di massima allerta contro attentati terroristici[479], era infatti evidente l'esigenza di riesaminare la disciplina della c.d. *data retention* alla luce dei principi di necessità e proporzionalità, tenendo in considerazione l'interesse di sicurezza nazionale e il buon funzionamento del mercato interno, nonché il diritto fondamentale alla protezione dei dati personali.

---

[477] Si veda, ad esempio, COM (2011) 225 definitivo, 10, tab.2. avente ad oggetto l'accessibilità dei dati, secondo cui quattordici Stati membri includono tra le autorità competenti gli organi di sicurezza nazionale e le forze militari, sei Stati membri le autorità fiscali e/o doganali e tre stati membri i servizi di frontiera. In undici Stati membri, occorre l'autorizzazione del giudice per procedere all'accesso e all'estrazione dei dati conservati. In tre Stati membri l'autorizzazione dell'autorità giurisdizionale è prevista soltanto in alcuni casi predeterminati. Secondo quattro legislazioni nazionali, l'autorizzazione necessaria per disporre l'accesso ai dati proviene da un'autorità di alto livello.
Sui tempi di archiviazione si veda invece COM (2011) 225 definitivo, 15, tab.3. secondo cui quindici Stati membri prevedono un unico lasso di tempo valido per tutte le categorie di dati. In Polonia è previsto un periodo di conservazione pari a due anni, dieci Stati indicano invece un anno (Bulgaria, Danimarca, Estonia, Grecia, Spagna, Francia, Paesi Bassi, Portogallo, Finlandia, Regno Unito e tre indicano sei mesi (Cipro, Lussemburgo, Lituania). Solo cinque Stati membri hanno previsto una differenziazione dei dati di archiviazione in base alla tipologia di dati o alla gravità dei reati per cui si procede. Infine, il Belgio non ha previsto un periodo di conservazione specifico per i dati che rientrano nel raggio di applicazione della direttiva.

[478] Si richiama l'intervento di Peter Hustinx, allora Garante europeo per la protezione dei dati personali, alla conferenza «Taking on the Data Retention Directive» del 3 dicembre 2010. Si veda COM (2011) 225 definitivo, 33, nota 126.

[479] Sul punto si veda Cap I.

In conclusione, la Commissione europea si impegnava nel proporre una revisione del quadro giuridico vigente in materia di conservazione dei dati focalizzandosi sui seguenti aspetti: a) predisporre una armonizzazione del quadro giuridico attuale ed una eventuale riduzione del periodo di archiviazione dei dati; b) garantire un controllo indipendente sulle richieste d'accesso ai dati; c) assicurare la proporzionalità dell'intero processo di immagazzinamento, estrazione e uso dei dati.

La maggior parte di tali argomenti ricorrono nella giurisprudenza della Corte di Giustizia che si è espressa sull'argomento a partire dall'epocale[480] sentenza *Digital Rights*. Tale pronuncia è stata emessa in un momento storico delicato in cui il ricorso a mezzi di ricerca della prova ad "alto contenuto tecnologico"[481], tra cui l'accessibilità a dati di traffico telefonico e telematico, viene finalmente subordinato non soltanto alle esigenze di accertamento dei reati ma soprattutto alla tutela dei diritti inviolabili dei cittadini.

Se prima del trattato di Lisbona, la Corte di Lussemburgo aveva dato una visibilità ridotta alla tutela dei dati personali ai sensi dell'art. 8 CDFUE, a seguito della riforma del 2009, si è impegnata nella valorizzazione di tale diritto primario, quale parametro di legittimità del diritto derivato europeo. La Corte ha recepito le istanze provenienti dai tribunali nazionali, elevandosi a garante ultimo del principio di proporzionalità e necessità della normativa comunitaria e nazionale in tema di conservazione di dati di traffico. Tale inedita "vocazione costituzionale" ha dato luogo ad un formante giurisprudenziale in materia[482]. Ha, inoltre, contribuito a ridefinire la portata applicativa degli articoli 7 e 8 della Carta di Nizza, a conferma del ruolo che tale documento ha progressivamente assunto nel processo di integrazione e costituzionalizzazione dell'Unione europea.

Come si è detto pocanzi, la prima tappa di indubbio rilievo del processo di affermazione della Corte di Lussemburgo come "giudice dei diritti"[483] in materia di

---

[480] L'espressione è di FLOR, *La Corte di giustizia considera la direttiva europea 2006/24 sulla cd*. "data retention" *contraria ai diritti fondamentali. Una lunga storia a lieto fine?* in *Dir. Pen. contemp,* 2014, 178.

[481] Sul punto FLOR., *Investigazioni ad alto contenuto tecnologico e tutela dei diritti. Fondamentali della persona nella recente giurisprudenza del Bundesverfassungsgericht,* cit., 360.

[482] Cfr. ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, *cit.*, 67.

[483] L'espressione è di TRUCCO, *Data retention: la Corte di Giustizia si appella alla Carta UE dei diritti fondamentali*, in *Giur. it*., 2014, 1580.

data retention è rappresentata dalla sentenza dell'8 aprile 2014 emessa nel caso *Digital Rights Ireland* e *Seitlinger* e altri[484], di cui seguirà una puntuale esegesi.

8. Il caso *Digital Rights Ireland Ltd.* (2014).

La storica pronuncia si è occupata delle cause riunite[485] C-293/ 12 e C-594/12, aventi ad oggetto due domande di pronuncia pregiudiziale proposte rispettivamente dalla *High Court* (Irlanda)[486] e dal *Verfassungsgerichtshof*[487] (Austria) ai sensi dell'art. 267 TFUE[488]. Entrambe vertevano sulla validità della direttiva 2006/24/CE.

La prima causa (C-293/12) ha origine dal ricorso[489] presentato dalla *Digital Rights Ireland Ltd – DRI*[490], società dedita alla sensibilizzazione dei diritti umani nell'era delle comunicazioni digitali, contro due ministri del governo irlandese[491], il comandante della polizia e l'*Attorney General*[492] della Repubblica d'Irlanda. Mediante

---

[484] Si fa riferimento alla Corte giust. UE, Gr. Sez., sent. 8 aprile 2014, *Digital Rights*, in *www.eur-lex.europa.eu*.

[485] Le due cause sono state riunite in vista della fase orale del procedimento e della decisione finale con atto del Presidente Della Corte del 6 giugno 2013. Cfr. § 22 Sent. *de qua*.

[486] Nel sistema giudiziario irlandese la *High Court* ha competenza originaria su tutte le questioni di diritto e di fatto, in materia civile e penale. Inoltre, si occupa delle questioni aventi ad oggetto la validità delle leggi rispetto alle disposizioni della Costituzione come nel caso di specie. Per un maggior approfondimento sulla giurisdizione ordinaria irlandese si veda *www.e-justice.europa.ue*.

[487] Il *Verfassungsgerichtshof* (in acronimo *VfGH*) è la Corte costituzionale austriaca. Tra le tante funzioni che gli sono attribuite, compete a tale tribunale verificare la legittimità degli statuti, delle ordinanze e tutte le leggi secondarie.

[488] Il primo paragrafo dell'articolo 267 del Trattato sul funzionamento dell'Unione europea dispone così «La Corte di giustizia dell'Unione europea è competente a pronunciarsi, in via pregiudiziale: a) sull'interpretazione dei trattati; b) sulla validità e l'interpretazione degli atti compiuti dalle istituzioni, dagli organi o dagli organismi dell'Unione». Quando una questione avente ad oggetto uno dei due punti viene sollevata davanti ad un organo giurisdizionale nazionale, il giudice di merito può procedere alla sospensione del giudizio pendente e rivolgersi alla CGUE. Mediante tale rinvio pregiudiziale si mette in moto una procedura che esalta il principio di cooperazione giudiziaria tra il giudice dell'Unione e i giudici nazionali. Nel rispetto delle competenze reciproche, la Corte di Lussemburgo è chiamata a pronunciarsi sull'interpretazione o sulla validità di un atto secondario dell'Ue. Per un approfondimento sulla procedura in esame si veda STROZZI, MASTROIANNI, *Diritto dell'Unione europea. Parte istituzionale*, Torino, 2020, 412 ss.

[489] Il ricorso è stato presentato dinanzi alla *High Court* l'11 agosto 2006.

[490] Sul sito *www.digitalrights.ie*, che si invita a consultare, figura che la società «is dedicated to defending Civil, Human and Legal rights in a digital age». Nel ricorso, la *Digital Rights Ireland* ha precisato di essere proprietaria di un telefono cellulare registrato un paio d'anni prima del procedimento e in uso a partire da quella data.

[491]Nello specifico, vengono coinvolti nella suddetta controversia il *Minister for Communications, Marine and Natural Resources* (che può essere tradotto come il ministro per le comunicazioni e le risorse marine e naturali) e il *Minister for Justice, Equality and Law Reform* (Il ministro per la giustizia, l'equità e le riforme giuridiche).

[492] Nell'ordinamento irlandese, l'*Attorney General* è il Procuratore generale. Tale figura non è un membro del Governo ma partecipa alle riunioni del gabinetto al consiglio dei ministri. In sintesi, riveste la funzione di consulente legale per il Governo in carica. Sul punto si veda, *www.attorneygeneral.ie*.

tale istanza, si chiedeva l'annullamento della direttiva sopracitata[493] e del *Criminal Justice (Terrorist Offences) Act 2005*[494], nella parte in cui imponeva ai fornitori di servizi una conservazione dei dati di traffico e di ubicazione generalizzata. Secondo la ricorrente, entrambi gli atti risultavano in contrasto sia la Costituzione irlandese sia con la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Ritenendo di non poter dirimere la controversia senza che prima fosse esaminata la validità della Direttiva 2006/24/CE, la *High Court* sospendeva il procedimento in atto e sottoponeva una serie di questioni pregiudiziali al vaglio della CGUE[495].

In primo luogo,[496] la Corte di Giustizia era chiamata a verificare se la limitazione dei diritti degli utenti nell'ambito delle comunicazioni elettroniche, derivante dal combinato disposto degli articoli 3, 4, 6[497] della direttiva fosse compatibile con l'art. 5, paragrafo 4, del TUE[498]. Si riteneva, infatti, che la conservazione generalizzata dei dati per un lungo periodo non fosse proporzionata al perseguimento di obiettivi comunitari, nel caso di specie all'accertamento e al perseguimento di reati gravi per garantire il corretto andamento del mercato interno dell'Ue.

Inoltre, la Corte era chiamata a valutare la compatibilità della direttiva con il diritto dei cittadini di circolare e soggiornare liberamente nel territorio dell'Unione ai

---

[493] Si veda Corte giust. UE, Grande Sezione, 10 febbraio 2009, *Irlanda c. Parlamento europeo*, causa C-301/06, in *www.curia.europa.eu* ed il commento di FABBRINI, *Lotta al terrorismo e tutela dei dati personali alla luce della sentenza Irlanda c. Parlamento e Consiglio*, in *Quaderni Costituzionali*, 2009, 419 ss.

[494] Il *Criminal Justice (Terrorist Offences) Act* è un atto di diritto interno, emanato nel giugno 2005 con l'obiettivo di emendare alcune diposizioni di diritto penale sostanziale. Nella controversia in esame si fa riferimento la Parte 2 interamente dedicata alla soppressione di gruppi di matrice terroristica. È possibile consultare *online* il testo di tale atto legislativo sul sito *www.irishstatutebook.ie*.

[495] NINO, *L'annullamento del regime della conservazione dei dati di traffico nell'Unione europea da parte della Corte di giustizia UE: prospettive ed evoluzioni future del sistema europeo di* data retention, in *Diritto dell'Unione Europea,* 2014, 803.

[496]Cfr. Corte giust. UE, Gr. Sez., 8 aprile 2014, *Digital Rights Ireland*, cit., punto 18.

[497] L'articolo 3 della direttiva 2006/24/CE dettava un obbligo di conservazione dei dati in deroga agli articoli 5, 6 e 9 della direttiva 2002/58/CE. L'articolo 4, rubricato l'«accesso dei dati», stabiliva che gli Stati membri potessero adottare procedure per garantire l'acquisizione dei dati da parte delle autorità nazionali competenti. Ai sensi dell'articolo 6, si stabiliva che il periodo di archiviazione non potesse essere inferiore a sei mesi e superiore a due anni.

[498] L'articolo 5, paragrafo 4, del TUE dispone che «In virtù del principio di proporzionalità, il contenuto e la forma dell'azione dell'Unione si limitano a quanto necessario per il conseguimento degli obiettivi dei trattati».

sensi dell'articolo 21 del TFUE[499]. Si chiedeva poi di verificare la legittimità della direttiva alla luce dell'articolo 7 della Carta di Nizza[500], del diritto alla protezione dei dati (art. 8 CDFUE), del diritto alla libertà di espressione (art. 11. CDFUE)[501] e del diritto ad una buona amministrazione contemplato dall'articolo 41[502] della Carta.

Nella seconda causa (C-594/12), il sig. *Seitlinger*[503] sollevava dinanzi al *Verfassungsgerichtshof* un ricorso dal contenuto simile al primo, richiedendo l'annullamento dell'articolo 102-*bis* della legge sulle comunicazioni austriaca (*Telekommunikationgesetz 2003*)[504] volta ad attuare le disposizioni della direttiva 2006/24/CE nell'ordinamento interno. In particolare, si lamentava l'incostituzionalità della norma di diritto interno in quanto in contrasto con il diritto fondamentale alla protezione dei dati personali. Anche in questo caso, la Corte austriaca decideva di sospendere il giudizio e di sottoporre alla Corte di Lussemburgo numerose questioni in merito alla validità della direttiva 2006/24/CE.

La prima era del tutto analoga a quelle prospettate nel precedente ricorso, in quanto si richiedeva di esaminare la legittimità della direttiva alla luce degli articoli 7, 8, 11 della Carta di Nizza.

Di seguito, il *Verfassungsgerichthof* sottoponeva alla Corte un'ulteriore questione relativa all'interpretazione dei Trattati. In particolare, si domandava quale fosse il rapporto intercorrente tra gli artt. 8 e 52[505] della Carta da una parte e la direttiva

---

[499] L'articolo 21, paragrafo 1, del TFUE prevede che «Ogni cittadino dell'Unione ha il diritto di circolare e di soggiornare liberamente nel territorio degli Stati membri, fatte salve le limitazioni e le condizioni previste dai trattati e dalle disposizioni adottate in applicazione degli stessi».

[500] Sul punto si veda *supra*.

[501] L'art. 11, par 1, della Carta di Nizza prevede che «Ogni persona ha diritto alla libertà di espressione. Tale diritto include la libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera».

[502] L'articolo 41, paragrafo 1, della Carta di Nizza dispone che «Ogni persona ha diritto a che le questioni che la riguardano siano trattate in modo imparziale ed equo ed entro un termine ragionevole dalle istituzioni, organi e organismi dell'Unione».

[503] Insieme al sig. *Seitlinger* altri 11.000 ricorrenti presentavano congiuntamente ricorso dinanzi alla Corte costituzionale austriaca per richiedere l'annullamento dell'articolo sopracitato.

[504] Il *Telekommunikationsgesetz 2003,* traducibile in italiano con l'espressione "diritto delle telecomunicazioni", è atto legislativo di diritto interno contenente una serie di previsioni nell'ambito dei servizi elettronici e digitali. L'articolo 102-*bis* richiamato nel testo è stato introdotto nella legge federale tedesca sulle comunicazioni soltanto nel 2011.

[505] Sottolinea come i limiti posti dagli articoli 8, par. 2 CEDU e 52, par. 1 Carta siano equipollenti. L'art. 8, par. 2 CEDU rispetto alla Carta aggiunge che la limitazione dei diritti fondamentali deve essere «necessaria in una società democratica». Secondo la CEDU per giustificare la misura derogatoria risulterebbe necessario rinvenire un bisogno sociale che metta in crisi il funzionamento stesso della società. Per un approfondimento sul punto si veda CAGGIANO, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione,* in *Medialaws – Rivista dir. media*, 2018, fasc. 2, 70, nota n.16.

95/46/CE[506] e il regolamento 45/2001/CE[507] dall'altra. Tali norme di diritto derivato ponevano – e tuttora pongono, in parte – condizioni e limiti all'esercizio del diritto fondamentale alla protezione dei dati sancito dalla Carta. Il tribunale austriaco sottolineava, dunque, la necessità di valutare se gli atti sopra richiamati dovessero essere ritenuti equivalenti alle norme previste nella CDFUE per la valutazione dell'ammissibilità delle ingerenze sui diritti fondamentali coinvolti.

8.1 La decisione della Corte di Giustizia.

Nel pronunciarsi sulle questioni pregiudiziali appena riportate, la Corte ha innanzitutto rilevato che i dati di traffico archiviati ai sensi degli artt. 3, 4 e 5 direttiva 2006/24/CE consentivano di trarre precise conclusioni riguardo alle abitudini giornaliere dei cittadini europei, ai luoghi di residenza permanente o temporanea, sui loro spostamenti e le loro attività nonché alle relazioni sociali da essi stabilite[508].

Di seguito, la Corte specificava che l'obbligo di archiviazione di tali informazioni incideva sull'esercizio della libertà di espressione degli abbonati o degli utenti a cui i dati si riferiscono ai sensi dell'articolo 11 della Carta. Sebbene la direttiva non avesse ad oggetto il "contenuto" delle conversazioni, questa risultava comunque in grado di incidere sull'utilizzo da parte degli interessati dei mezzi di comunicazione elettronica e sulle modalità da loro prescelte per trasmettere informazioni[509].

Inoltre, i giudici rilevavano che l'attività di accesso e di estrazione dei dati da parte delle autorità competenti costituiva di per sé un'interferenza dei diritti fondamentali tutelati dagli articoli 7 e 8 della Carta. Ciò risultava indipendentemente dal fatto che le informazioni relative alla vita privata avessero o meno un carattere "sensibile". In conformità rispetto a quanto affermato dall'Avvocato Generale nelle

---

[506] Sul punto si veda *supra.*

[507] Si fa riferimento al Regolamento n. 45/2001 del Parlamento europeo e del Consiglio del 18 dicembre 2000 «concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati». Tale atto è ancora in vigore e può essere consultato sempre presso il sito *www.eur-lex.europa.eu*.

[508] Nello stesso modo l'Avvocato generale riteneva che tali dati «qualificati» e «presi nel loro complesso» fossero in grado fornire precisi elementi riguardo alla vita privata e alla personalità degli utenti. Sul punto si veda Conclusioni dell'Avv. Gen. UE *Pedro Cruz Villalón*, presentate il 12 dicembre 2013, nelle cause riunite C-293/12 e C-594/12, *Digital Rights Ireland e Seitlinger*, cit. 74. Per prendere visione del testo integrale del documento citato v. sempre *www.eur-lex.europa.eu.*

[509] Cfr. Corte giust. UE, Gr. Sez., sent. 8 aprile 2014, *cit.*, punto 28.

sue conclusioni[510], la Corte riteneva che tale ingerenza doveva essere considerata particolarmente grave, in quanto veniva – e tuttora viene – effettuata senza che gli interessanti ne siano preliminarmente informati. Ciò poteva ingenerare nei cittadini europei la sensazione che la loro vita fosse sottoposta a sorveglianza permanente[511].

Una volta constatato che la direttiva 2006/24/CE realizzava una compressione dei diritti previsti dagli artt. 7 e 8 della Carta di Nizza, la Corte considerava tale interferenza legittima soltanto nella misura in cui fossero rispettate le condizioni stabilite dall'articolo 52, paragrafo 1[512]. Sulla base di tali premesse, si predisponeva un'analisi di compatibilità della *data retention* con i requisiti previsti dalla norma sopracitata, per la prima volta presi in considerazione singolarmente[513].

Innanzitutto, i giudici verificavano che fosse rispettato il principio di legalità. Siffatto requisito risultava ampiamente soddisfatto in quanto la normativa presa in considerazione era contenuta in un atto legislativo di diritto derivato dell'Unione europea. Sul punto i giudici non si sono dilungati oltre.

---

[510] Cfr. Conclusioni dell'Avv. Gen. UE *Pedro Cruz Villalón, cit.,* punto 77 e 80.

[511] Sul punto, si veda quanto già affermato dal *Bundesverfassungsgericht.*

[512] L'articolo 52, rubricato «Portata e interpretazione dei diritti e dei principi» della Carta di Nizza dispone che:

«1. 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.

2. I diritti riconosciuti dalla presente Carta per i quali i trattati prevedono disposizioni si esercitano alle condizioni e nei limiti dagli stessi definiti.

3. Laddove la presente Carta contenga diritti corrispondenti a quelli garantiti dalla Convenzione europea per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali, il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta convenzione. La presente disposizione non preclude che il diritto dell'Unione conceda una protezione più estesa.

4. Laddove la presente Carta riconosca i diritti fondamentali quali risultano dalle tradizioni costituzionali comuni agli Stati membri, tali diritti sono interpretati in armonia con dette tradizioni.

5. Le disposizioni della presente Carta che contengono dei principi possono essere attuate da atti legislativi e esecutivi adottati da istituzioni, organi e organismi dell'Unione e da atti di Stati membri allorché essi danno attuazione al diritto dell'Unione, nell'esercizio delle loro rispettive competenze, esse possono essere invocate dinanzi a un giudice solo ai fini dell'interpretazione e del controllo di legalità di detti atti.

6. Si tiene pienamente conto delle legislazioni e prassi nazionali, come specificato nella presente Carta.

7. I giudici dell'Unione e degli Stati membri tengono nel debito conto le spiegazioni elaborate al fine di fornire orientamenti per l'interpretazione della presente Carta».

[513] La novità del percorso argomentativo della Corte che ha proceduto separatamente all'analisi del contenuto essenziale dei diritti fondamentali e, in seguito, a quello relativo alla proporzionalità della misura viene sottolineato da POLLICINO, *Diritto all'oblio e conservazione dei dati. La Corte di giustizia a piedi uniti: verso un* digital right to privacy, in *Giur. Cost*., 2014, 2949 e ss.

In secondo luogo, la Corte si accertava che l'attività di conservazione dei dati di traffico non pregiudicasse *ex se* il «contenuto essenziale» dei diritti e delle libertà coinvolte. Sul punto, la Corte considerava illeso il c.d. «nucleo duro» del diritto fondamentale al rispetto della vita privata previsto dall'articolo 7, in quanto la direttiva 2006/24/CE permetteva di venire a conoscenza soltanto dei "dati esterni" e non del contenuto della comunicazione. Inoltre, riteneva che non fosse pregiudicato nemmeno il contenuto dell'articolo 8 della Carta, grazie a quanto stabilito nell'art. 7[514] della direttiva 2006/24/CE. Siffatta disposizione imponeva ai fornitori di servizi di comunicazione accessibili al pubblico di rispettare misure di protezione e sicurezza dei dati disposte dagli Stati membri. Tra di esse, rientravano strumenti tecnici e organizzativi diretti ad evitare la cancellazione accidentale e illecita dei dati, la compromissione della loro integrità mediante alterazione non autorizzata, nonché a garantire che essi fossero distrutti alla fine del periodo di conservazione[515]. Mediante tali strumenti, il legislatore comunitario si accertava che non fosse del tutto compromesso il diritto alla protezione dei dati di carattere personale.

In terzo luogo, i giudici procedevano a verificare che la limitazione dei diritti fondamentali rispondesse ad «un interesse generale riconosciuto dall'Unione». Ai sensi dell'articolo 1, la direttiva si proponeva l'obiettivo di armonizzare le disposizioni degli Stati membri in tema di *data retention* nell'ottica di garantire la disponibilità dei dati per esigenze di indagine, di accertamento e perseguimento dei reati gravi. In senso lato, i giudici individuavano il fine ultimo dell'atto nell'esigenza di contribuire alla lotta contro la criminalità grave e il terrorismo internazionale a tutela della pubblica

[514] Per agevolare una maggiore comprensione di quanto *supra*, si ritiene utile riportare l'art. 7 della direttiva 2006/24/CE nella sua interezza:
«Fatte salve le disposizioni adottate in conformità della direttiva 95/46/CE e della direttiva 2002/58/CE, ogni Stato membro provvede a che i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione rispettino, come minimo, i seguenti principi di sicurezza dei dati per quanto concerne i dati conservati in conformità della presente direttiva:
a) i dati conservati sono della stessa qualità e sono soggetti alla stessa sicurezza e tutela dei dati in rete;
b) i dati sono soggetti ad adeguate misure tecniche e organizzative intese a tutelarli da una distruzione accidentale o illecita, da un'alterazione o perdita accidentale, da immagazzinamento, trattamento, accesso o divulgazione non autorizzati o illeciti;
c) i dati sono soggetti ad adeguate misure tecniche e organizzative intese a garantire che gli stessi possono essere consultati soltanto da persone appositamente autorizzate;
d) i dati vengono distrutti alla fine del periodo di conservazione, fatta eccezione per quelli consultati e conservati».
[515] Sul punto, si veda FLOR, *La Corte di giustizia considera la direttiva europea 2006/24 sulla cd.* "data retention" *contraria ai diritti fondamentali. Una lunga storia a lieto fine? cit*., 184.

sicurezza. Facendo perno sull'articolo 6 della Carta di Nizza, che assicura il diritto fondamentale alla libertà nonché alla "sicurezza" al fine del mantenimento della pace, la Corte riteneva incontestabile la sussistenza di un obiettivo di interesse generale dell'Unione[516].

Ciò posto, la Corte procedeva a verificare la sussistenza di un rapporto di proporzionalità tra l'ingerenza constatata e il legittimo interesse dell'Unione. Perché si potesse rispettare il principio di proporzionalità, secondo giurisprudenza costante[517], i giudici erano, infatti, tenuti a valutare sia l'«idoneità» sia la «necessità» della *data retention* rispetto all'obiettivo perseguito dalla direttiva 2006/24/CE.

In merito al primo requisito, la Corte sottolineava che le tecnologie informatiche e i mezzi di comunicazione elettronica possono risultare estremamente utili per le indagini penali. Nel caso di specie, la conservazione dei dati di traffico garantisce maggiori opportunità nell'accertamento di reati gravi e di allarme sociale. Tale strumento veniva, dunque, ritenuto «idoneo» a perseguire l'obiettivo di interesse generale[518]. Si constatava, però, che l'esigenza di garantire la pubblica sicurezza e il mantenimento della pace non legittima di per sé la conservazione dei dati di traffico così come prevista dalla direttiva 2006/24/CE. È, infatti necessario, verificare ulteriormente se siffatta misura in deroga al rispetto della vita privata si limitasse allo «strettamente necessario».

Affinché tale secondo requisito si possa considerare soddisfatto, la Corte rilevava che la normativa comunitaria deve prevedere regole «chiare e precise»[519] per proteggere i dati personali contro il rischio di abusi. La presenza di siffatti requisiti minimi risulta ancor più essenziale in quanto i dati di traffico sono soggetti ad un trattamento «automatico» che aumenta il rischio di trattamento illecito degli stessi.

---

[516]Cfr. Corte giust. UE, Gr. Sez., Digital Rights Ireland, sent. 8 aprile 2014, *cit.*, punto 42 in cui la Corte sottolinea come emerga da giurisprudenza costante che la lotta contro il terrorismo internazionale finalizzata al mantenimento della pace e alla pubblica sicurezza costituisca un obiettivo di interesse generale. In tal senso, richiama sentenze *Kadi e Al Barakaat*, C-402/05 P e C-415/05 P, punto 363, nonché *Al-Aqsa*, C-539/10 P e C-550/10 P, punto 130.

[517] Corte giust. UE, Gr. Sez., sent. 8 aprile 2014, *cit.*, punto 46 in cui la Corte richiama le sentenze *Afton Chemical*, C-343/09, punto 45; *Volker und Markus Schecke e Eifert*, punto 74; *Nelson* e a., C-581/10 e C-629/10, punto 71; *Sky Österreich*, C-283/11, punto 50, nonché Schaible, C-101/12, punto 29.

[518] A sostegno di tale tesi viene richiamato il Considerando 7 della direttiva 2006/24 che, a sua volta, fa rinvio, alle conclusioni del Consiglio «Giustizia e affari interni» del 19 dicembre 2002. In tale atto si sottolinea che i dati relativi all'uso dei mezzi di comunicazione elettronica costituiscono uno strumento particolarmente valido nella prevenzione, indagine, accertamento e perseguimento dei reati.

[519] Corte giust. UE, Gr. Sez., sent. 8 aprile 2014, *Digital Rights Ireland*, cit., punto 54.

Inoltre, la Corte rilevava che la direttiva estendeva la c.d. *data storage* a tutti i dati di traffico, con qualsiasi mezzo di comunicazione elettronica essi fossero generati. Ciò dava luogo ad un'operazione di controllo «generalizzata» nei confronti di tutti gli utenti, indipendentemente dal fatto che questi ultimi venissero a trovarsi, anche indirettamente, in una situazione che possa dare avvio ad un procedimento penale. Inoltre, dall'assenza di deroghe, deduceva che la conservazione dei dati si applica anche a persone vincolate dal segreto professionale in base alle norme di volta in volta vigenti nell'ordinamento nazionale.

In aggiunta, la direttiva non prevedeva la sussistenza di un «nesso oggettivo» tra i dati oggetto dell'obbligo di archiviazione e il reato o la minaccia per la sicurezza pubblica[520]. L'attività di archiviazione non veniva circoscritta ad un periodo di tempo determinato né ad una determinata area o cerchia di persone che risulta in qualche modo coinvolte in un crimine grave.

Alla suddetta mancanza di elementi di natura sostanziale, si aggiungeva l'assenza di condizioni procedurali per l'accesso ai dati e per il successivo utilizzo nell'ambito di procedimenti penali. L'articolo 4 della direttiva 2006/24 lasciava, infatti, agli Stati membri il compito di definire l'*iter* procedurale e i requisiti sostanziali per l'acquisizione dei dati da parte delle autorità nazionali. La normativa europea non prevedeva né alcun criterio che permettesse di delimitare il numero di persone autorizzate ad accedere ai dati di traffico né subordinava lo stesso ad un previo controllo giurisdizionale o di una autorità amministrativa indipendente[521].

In merito alla durata di conservazione dei dati, l'articolo 6 della direttiva Frattini prevedeva un lasso di tempo che oscillava tra i sei e i ventiquattro mesi, senza precisare che la determinazione del periodo dovesse basarsi su criteri oggettivi per garantire la limitazione allo «stretto necessario»[522].

Per di più, con riferimento alla sicurezza e alla protezione dei dati oggetto dell'obbligo di archiviazione la direttiva 2006/24/CE non prevedeva tutele sufficienti – e in linea con quanto stabilito dagli articoli 7 e 8 della Carta di Nizza – che permettessero di assicurarne una protezione efficace. Non era disposta l'adozione di

---

[520] Cfr. COLOMBO, "Data retention" *e Corte di giustizia: riflessioni a prima lettura sulla declaratoria di invalidità della direttiva: riflessioni a prima lettura sulla declaratoria di invalidità della direttiva 2006/24/CE*, in *Cass. pen*., 2014, 2705.
[521] Cfr. Corte giust. UE, Gr. Sez., 8 aprile 2014, *Digital Rights Ireland,* cit., punto 38.
[522] Cfr. Corte giust. UE, Gr. Sez., 8 aprile 2014, *Digital Rights Ireland,* cit., punto 52.

precauzioni per evitare rischi di abuso, accesso illegale o uso non autorizzato né per preservare l'integrità e la riservatezza dei dati acquisiti. L'articolo 7 della direttiva autorizzava i gestori di servizi a seguire criteri di mera economicità[523] e di tener conto dei costi di attuazione delle misure nel determinare gli *standard* di sicurezza da applicare ai dati[524].

Infine, la direttiva sopracitata non richiedeva che i dati di traffico dovessero essere conservati all'interno del territorio dell'UE. Ciò non consentiva di ritenere pienamente garantito il controllo da parte di un'autorità indipendente, espressamente richiesto dall'articolo 8, paragrafo 3 della Carta di Nizza.

Alla luce delle osservazioni suesposte, la Corte riteneva che la direttiva 2006/24 realizzava un'ingerenza nei diritti fondamentali 7 e 8 della Carta di particolare gravità, senza che questa fosse regolamentata con disposizioni chiare secondo il criterio dello "strettamente necessario". A causa dell'insussistenza di tale secondo requisito, si constatava la violazione da parte del legislatore dell'Unione del principio di proporzionalità imposto dall'articolo 52, paragrafo 1, della Carta.

Ritenendo non necessario procedere all'esame delle restanti questioni pregiudiziali[525], la Corte dichiarava l'invalidità *ex tunc*[526] della direttiva 2006/24[527]

[523] Già la Corte costituzionale tedesca aveva sottolineato in senso critico il c.d. "criterio di economicità" nella citata sentenza del 2 marzo 2010 sulla *data retention*. Sul punto si rinvia a FLOR, *Investigazioni ad alto contenuto tecnologico e tutela dei diritti fondamentali della persona nella recente giurisprudenza del Bundesverfassungsgericht*, cit., 374.
[524] Corte giust. UE, Gr. Sez., sent. 8 aprile 2014, *Digital Rights Ireland,* cit., punto 54.
[525] La Corte ha ritenuto infatti superfluo esaminare la compatibilità della direttiva 2006/24 rispetto all'articolo 11 della Carta. Cfr. Corte giust. UE, Gr. Sez., 8 aprile 2014, *Digital Rights Ireland,* cit., punto 70.
[526]Sul punto i giudici non si sono conformati alle indicazioni dell'Avvocato Generale Cruz Villalón, che aveva raccomandato alla Corte di sospendere gli effetti della dichiarazione d'invalidità per consentire al legislatore dell'Unione di adottare le misure necessarie per porvi rimedio entro un tempo ragionevole (Cfr. Conclusioni del 12 dicembre 2013, punto 158). In tal senso si veda ARENA, *La Corte di Giustizia sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento*, *cit.*, 2014, 722.
[527] I giudici si sono pronunciati per l'invalidità della direttiva nonostante nel corso del procedimento siano intervenuti a sostegno della validità della direttiva le tre istituzioni del dell'Unione europea e ben 8 governi nazionali tra cui l'Italia.

nella sua interezza[528] in quanto incidente in modo sproporzionato sul diritto al rispetto della vita privata e sulla protezione dei dati personali[529].

La "storica" pronuncia, di cui si sono analizzati i passaggi essenziali, ha ribadito in modo definitivo che la semplice raccolta dei dati che riguardano l'individuo in genere – e in specie i dati di traffico – costituisce di per sé un'ingerenza nella "sfera privata" dell'individuo[530]. Siffatta attività integra inoltre un «trattamento» dei dati di carattere personale che, come tale, deve necessariamente rispettare le condizioni prescritte dall'art. 8, par. 2, CFDUE.

Per giungere a tale conclusione, i giudici hanno realizzato un giudizio di bilanciamento tra la tutela dei diritti fondamentali e l'interesse pubblico di accertamento dei reati. Non è la prima volta che la Corte di Lussemburgo ha tentato di raggiungere un equilibrio tra esigenze opposte e, allo stesso tempo, incidenti sull'esercizio dei diritti della persona in ambito digitale[531]. Nella sentenza di cui trattasi, però, la CGUE ha sottolineato con vigore che i primi debbano essere oggetto di tutela privilegiata da parte del legislatore europeo e nazionale. Per non dover rinunciare *in toto* all'utilizzo di strumenti tecnologici efficaci nella prevenzione e nell'accertamento di reati gravi, è necessario che sia garantito il rispetto del loro «nucleo essenziale».

---

[528]La decisione della Corte di caducare l'atto legislativo *in toto* ha pochissimi precedenti. Sebbene si fosse già accertato in precedenti pronunce l'incompatibilità tra gli atti di diritto derivato e i principi fondamentali dell'Ue, in tali occasioni i giudici si erano limitati a dichiarare l'invalidità di singole disposizioni e non di tutta la direttiva (cfr. Corte giust. 1° marzo 2011, *Association Belge des Consommateurs Test-Achats ASBL* e altri c. *Conseil des ministres*, causa C-236/09; Corte giust., 9 novembre 2010, *Volker* und *Markus Schecke GbR* e *Hartut Eifert* c. *Land Hessen*, cause riunite C-92/09 e C-93/09). Sul punto si veda ARENA, *La Corte di Giustizia sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento*, cit, 722.

[529] Cfr. IOVENE, Data retention *tra passato e futuro. Ma quale presente?* in *Cass. Pen*., 2014, 4274.

[530] Così ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, *cit.*, 64.

[531]È da segnalarsi la sentenza *Google Spain SL* e *Google Inc. contro Agencia Española de Protección de Datos (AEPD)* e *Mario Costeja González* del 13 maggio 2014 (C-131/12), la quale ha affermato la prevalenza dei diritti tutelati dagli artt. 7 e 8 della Carta rispetto alla libertà di espressione e agli interessi economici dei *providers,* privilegiando in questo modo la posizione giuridica della persona interessata. Secondo la Corte di Giustizia, i diritti fondamentali sopracitati prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse del pubblico degli utenti a ricavare informazioni mediante una ricerca *online* relativa ad una persona determinata, a cui è riconosciuto il "diritto all'oblio". Per un maggior approfondimento sul punto si veda FINOCCHIARO, *La giurisprudenza della Corte di giustizia in materia di dati personali da "Google Spain" a "Schrems"* in Il Diritto dell'informazione e dell'informatica, 2015, fasc. 4-5, 780 ss.

Ciò posto, la sentenza *Digital Rights Ireland* ha lasciato una serie di questioni aperte relativamente alle normative di diritto interno introdotte dagli Stati membri[532] per recepire la direttiva 2006/24/CE giudicata invalida. In particolare, ci si è domandato[533] se la caducazione dell'atto di diritto derivato da parte della Corte di Giustizia avesse, di fatto, prodotto la fuoriuscita delle norme in materia di *data retention* dall'ambito di applicazione del diritto comunitario. Tale interrogativo non era privo di risvolti pratici, perché, in caso di risposta affermativa, le discipline di diritto nazionale sarebbero state private del collegamento del diritto dell'Unione[534] ed esonerate dal rispetto della Carta di Nizza, come previsto dall'articolo 51[535].

A contrario, la Corte di Lussemburgo ha chiarito[536] che la c.d. direttiva Frattini costituiva una *lex specialis*[537] rispetto alla direttiva 2002/58, relativa alla vita privata e alle comunicazioni elettroniche, il cui art. 15, paragrafo 1[538] prevede che gli Stati

---

[532] Tra l'altro la questione riguardava direttamente anche l'Italia che, come si è visto, ha trasposto la direttiva 2006/24 con il decreto legislativo 30 maggio 2008, n. 109 (Cfr. Cap. I § 3.5).

[533] Cfr. FLOR, *La Corte di giustizia considera la direttiva europea 2006/24 sulla cd*. "data retention" *contraria ai diritti fondamentali. Una lunga storia a lieto fine?* in *Dir. Pen. contemp.., 2014*, fasc. 2, 178.

[534] Per la Corte di giustizia, la nozione di norma di recepimento dell'Unione europea implica «un collegamento di una certa consistenza» tra la misura nazionale e la normativa dell'Unione. In tal senso v. STROZZI, MASTROIANNI, *Diritto dell'Unione europea. Parte istituzionale*, *cit.*, 296 ss.

[535] L'Articolo 51 della Carta di Nizza, rubricato «Ambito di applicazione» prevede che**:**

«1. Le disposizioni della presente Carta si applicano alle istituzioni, organi e organismi dell'Unione nel rispetto del principio di sussidiarietà, come pure agli Stati membri esclusivamente nell'attuazione del diritto dell'Unione. Pertanto, i suddetti soggetti rispettano i diritti, osservano i principi e ne promuovono l'applicazione secondo le rispettive competenze e nel rispetto dei limiti delle competenze conferite all'Unione nei trattati.

2. La presente Carta non estende l'ambito di applicazione del diritto dell'Unione al di là delle competenze dell'Unione, né introduce competenze nuove o compiti nuovi per l'Unione, né modifica le competenze e i compiti definiti nei trattati».

[536] Si veda in tal senso Corte giust. 19 aprile 2012, *Bonnier Audio AB e altri c. Perfect Communication Sweden AB***,** C-461/10, punto 43. È possibile consultare il testo della sentenza sul sito *www.curia.europa.eu*.

[537] L'espressione è utilizzata da ARENA, *La Corte di Giustizia sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento*, *cit.*, 723.

[538]L'art. 15, paragrafo 1, della direttiva 2002/58/CE prevede che:

«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/CE, 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 comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea».

membri possano adottare misure di conservazione dei dati di traffico in quanto compatibili con i «principi generali del diritto comunitario».[539]Sulla base di tali osservazioni, è indubbio che le misure nazionali di *data retention* rientrino ancora oggi nell'ambito di applicazione della direttiva e-*Privacy* e che debbano essere conformi ai principi espressi dalla Carta di Nizza.

Da tale premessa, scaturiva un'altra questione su cui la sentenza in esame non era stata in grado di fare chiarezza. In dottrina e in giurisprudenza, sussistevano infatti numerosi dubbi circa la compatibilità con il diritto dell'Unione delle normative nazionali di conservazione dei dati di traffico emanate per recepire la direttiva dichiarata invalida.

Tale situazione di incertezza[540] veniva alimentata dalla posizione piuttosto ambigua assunta dalla Commissione europea nel comunicato stampa successivo all'emanazione della sentenza in oggetto. In tale atto[541], si affermava la necessità di emendare le normative interne soltanto nella parte in cui risultavano in contrasto con le disposizioni della Corte di Giustizia. Inoltre, la Commissione rimarcava che la dichiarazione di invalidità della direttiva non aveva in alcun modo privato gli Stati membri del potere di disporre misure interne di conservazione dei dati di traffico.

In merito a tale questione, altrettanto fumoso era il parere dell'Avvocato Generale Cruz Villalón il quale affermava[542] che, in alcuni casi, gli Stati membri avevano posto rimedio alle insufficienti garanzie previste dalla direttiva Frattini in sede di recepimento. Si ritenevano, così, potenzialmente ammissibili le disposizioni nazionali che avevano apportato correttivi alla direttiva in materia di accesso e acquisizione dei dati raccolti, attenuandone le criticità. *A contrario*, le normative nazionali che avevano "pedissequamente" riprodotto il contenuto della direttiva

[539] Per un maggior approfondimento sul tema si veda *supra*.
[540] Sulla base di quanto affermato, lo scenario era anche aggravato – ed è tuttora, in assenza di uno specifico intervento da parte del legislatore dell'Unione – dalla disomogeneità delle singole previsioni statali.
[541] Si fa riferimento Memo della Commissione europea rilasciato a *Bruxelles* in data 8 aprile 2014, recante «Frequently Asked Questions: The Data Retention Directive». In particolare all'altimo punto si afferma che «National legislation needs to be amended only with regard to aspects that become contrary to EU law after a judgment by the European Court of Justice. Furthermore, a finding of invalidity of the Directive does not cancel the ability for Member States under the e-Privacy Directive (2002/58/EC) to oblige retention of data». Per consultare il testo completo in lingua inglese si veda *www.ec.europa.eu.*
[542] Cfr. Conclusioni dell'Avv. Gen. UE *Pedro Cruz Villalón, cit.,* punto 157.

invalidata dovevano senz'altro ritenersi incompatibili con le garanzie sancite dalla Carta dei diritti.

Un altro punto lasciato irrisolto dai giudici riguardava le procedure di infrazione[543] avviate ai sensi dell'articolo 258 TFUE[544] dalla Commissione europea nei confronti degli Stati membri[545] che non avevano recepito la Direttiva 2006/24/CE. Alcune indicazioni sul punto erano state fornite in una seduta parlamentare dal Commissario Cecilia Malmström[546] che aveva annunciato l'intenzione della Commissione di ritirare i ricorsi proposti contro gli Stati inadempienti[547].

Inoltre, nello stesso intervento il Commissario demandava agli Stati membri il compito di stabilire se le normative nazionali, al pari della direttiva 2006/24/CE, incidessero in misura sproporzionata sulle garanzie fondamentali previste dalla Carta. Facendo leva sul principio di cooperazione giurisdizionale tra gli Stati membri, la Commissione sembrava dunque spogliarsi del suo ruolo di "custode dei trattati"[548] affidando il vaglio di compatibilità delle misure di conservazione dei dati di traffico alle Corti nazionali.

Siffatta presa di posizione della Commissione appariva condivisibile solo in parte[549], in quanto non era in grado di sgomberare del tutto il campo dalle incertezze in merito alle condizioni di compatibilità delle normative nazionali in tema di *data*

---

[543]Nell'ordinamento comunitario, mediante la procedura di infrazione, il giudice dell'Unione esercita un controllo sul rispetto da parte degli Stati membri, degli obblighi derivanti dalle regole dell'ordinamento comunitario. La sua funzione è quella di ristabilire la legalità all'interno dell'Unione, dopo che siano risultati insufficienti gli altri strumenti per porre fine alla violazione. Per un maggior approfondimento sul punto si veda STROZZI, MASTROIANNI, *Diritto dell'Unione europea. Parte istituzionale*, *cit.*, 344 ss.

[544] L'articolo 258 del TFUE prevede che*:* «La Commissione, quando reputi che uno Stato membro abbia mancato a uno degli obblighi a lui incombenti in virtù dei trattati, emette un parere motivato al riguardo, dopo aver posto lo Stato in condizioni di presentare le sue osservazioni. Qualora lo Stato in causa non si conformi a tale parere nel termine fissato dalla Commissione, questa può adire la Corte di giustizia dell'Unione europea».

[545] Si fa riferimento alle quattro procedure d'infrazione avviate nei confronti della Grecia (cfr. Corte giust., 26 novembre 2009, causa C-211/09); della Repubblica di Irlanda (cfr. Corte giust., 26 novembre 2009, causa C-202/09); della Svezia (cfr. Corte giust. 4 febbraio 2010, causa C-185/09); dell'Austria (Corte giust. 29 luglio 2010, causa C-189/09). Nel procedimento contro la Svezia la Commissione aveva anche ottenuto la condanna al pagamento di una somma forfettaria di 3 milioni di euro (Corte giust., 30 maggio 2013, Commissione c. Svezia, causa C-270/11).

[546] Si tratta della discussione del Parlamento del 16 aprile 2014 e all'intervento conclusivo del commissario Cecilia Malmström. Per visionare il verbale della discussione del parlamento richiamata si veda *www.europarl.europa.eu.*

[547] In effetti, la Commissione ha poi subito rispettato gli impegni presi, archiviando sia le cause in corso sia il procedimento ancora in fase di precontenzioso avviato contro il Belgio. Sul punto si veda ARENA, *La Corte di Giustizia sulla conservazione dei dati*, *cit*., 724.

[548] Per un approfondimento sulle funzioni della Commissione europea si veda *www.ec.europa.eu.*

[549] Sul punto, v. ARENA, *La Corte di Giustizia sulla conservazione dei dati*, *cit*., 724.

retention. In particolare, da alcune parti si è sottolineata la necessità che venissero definiti a livello comunitario dei parametri in base ai quali valutare in sede nazionale la compatibilità tra le disciplina di conservazione dei dati e i principi della Carta di Nizza.

9. Il caso *Tele2 Sverige AB e Watson* (2016).

Nel silenzio del legislatore europeo, le problematiche di cui *supra* sono state affrontate ancora una volta dalla Corte di Giustizia. La sentenza *Tele2 Sverige AB* c. l'Autorità svedese di Sorveglianza Poste e TLC[550], ha rappresentato infatti una tappa fondamentale nel percorso di rilettura dell'impianto normativo di diritto derivato in ambito di *data retention*. A poco più di un anno dal caso *Schrems*[551], i giudici sono tornati ad occuparsi del diritto alla *privacy* in ambito in ambito digitale e, in particolare, delle misure di conservazione dei dati di traffico.

Ancora una volta, la Corte di Giustizia è stata chiamata a trovare il punto di equilibrio tra il diritto alla protezione dei dati personali e le esigenze nazionali di contrasto ai reati gravi, in particolare nella lotta al terrorismo. La «grande difficoltà» dinanzi alla quale si sono trovati i giudici della Corte nell'affrontare la *vexata quaestio* è stata opportunamente sottolineata dall'avvocato generale, che ha aperto le sue conclusioni[552] con una citazione del politico statunitense *James Madison:*

«*If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great*

[550] Sul punto Corte giust. UE, Gr. Sez., sent. 21 dicembre 2016, *Tele2 Sverige*, *in www.curia.europa.eu*.
[551] Si tratta della sentenza della Corte di giustizia UE, 6 ottobre 2015, C-362/14, *Maximillian Schrems c. Data Protection Commissioner*. In tale pronuncia, si è dichiarata l'invalidità della decisione della Commissione con cui veniva siglato con gli Stati Uniti il c.d. *Privacy Shield System.* Siffatto accordo non risultava infatti compatibile con quanto affermato nella sentenza *Digital Rights*, secondo cui il trattamento dei dati personali dovesse essere improntato all'effettiva osservanza del principio di proporzionalità e di necessità. Per un maggior approfondimento sul contenuto della sentenza *de qua,* si veda ZENO-ZENCOVICH, *Intorno alla decisione nel caso "Schrems": la sovranità digitale e il governo internazionale delle reti di telecomunicazione,* in *Il Diritto dell'informazione e dell'informatica,* 2015, fasc. 4-5, 683-695.
[552] Si fa riferimento alle conclusioni presentate dall'avvocato generale *Henrik Saugmandsgaard Øe*, 19 luglio 2016 nelle Cause riunite C-203/15 e C-698/15. Per consultare il testo integrale del documento in esame si veda *www.curia.europa.eu*.

difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself»[553].

Il discorso del politico americano, risalente al 1788, risulta particolarmente efficace nel cogliere le implicazioni politiche della questione sottoposta alla Corte di Giustizia. Da una parte, la conservazione dei dati di traffico consente al governo di «controllare i governati», garantendo alle autorità competenti la possibilità di servirsi di informazioni utili per la repressione di reati di criminalità grave. Dall'altra, è opportuno «obbligare il governo a controllare se stesso» verificando che siano imposte limitazioni alla *data storage* nel rispetto del diritto alla *privacy* e di altri diritti di rango fondamentale.

Nella risoluzione della controversia *de qua*, ha giocato un ruolo fondamentale la sentenza dell'8 aprile 2014 nella causa *Digital Rights Ireland*, di cui la Corte ha in parte replicato l'*iter* argomentativo. Tra l'altro, l'importanza di tale pronuncia per la composizione delle cause in esame, rileva fin dalle questioni pregiudiziali che i giudici svedesi e britannici hanno sottoposto ai giudici dell'Unione. Come si vedrà meglio *infra*, nell'esaminare tali questioni dei giudici hanno realizzato uno scrutinio delle legislazioni nazionali secondo una prospettiva costituzionalmente orientata, volta a privilegiare la tutela degli artt. 7 e 8 della Carta di Nizza.

9.1 I due procedimenti principali.

La controversia è sorta sulla base dei rinvii pregiudiziali proposti rispettivamente dal *Kammarrätten i Stockholm* (Corte d'appello amministrativa di Stoccolma, Svezia) e dalla *Court of Appeal* dell'Inghilterra e del Galles nelle cause riunite C-203/15 e C-698/15[554]. Entrambe le domande vertevano sull'interpretazione

[553] Queste parole sono state scritte nel 1788 da *John Madison*, uno dei principali autori e uno dei 39 firmatari della Costituzione degli Stati Uniti redatta nel 1787. Tra il 1809 e il 1817, Madison divenne il quarto Presidente degli Stati Uniti. La citazione di cui sopra è riportata nel MADISON, *Federalist No. 51*, in HAMILTON, MADISON, JAY, GENOVESE, *The Federalist Papers*, New York, 2009, 120. Di seguito, si riporta la traduzione in italiano utilizzata nelle Conclusioni dell'avvocato generale, nota 2:
«Se gli uomini fossero angeli, non sarebbe necessario alcun governo. Se ci fossero angeli a governare gli uomini, non sarebbero necessari controlli esterni o interni sul governo. Nel dar forma a un governo di uomini su uomini, la grande difficoltà consiste in questo: occorre anzitutto consentire al governo di controllare i governati, e poi obbligare quest'ultimo a controllare se stesso».

[554] Le cause sono state riunite con decisione del presidente della Corte del 10 marzo 2016 ai fini della fase orale del procedimento e della sentenza. Cfr. Corte giust. UE, Gr. Sez., sent. 21 dicembre 2016, punto 61.

dell'articolo 15, paragrafo 1[555], della direttiva 2002/58/CE[556], alla luce degli articoli 7 e 8 nonché dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea[557].

Il primo procedimento principale (C-203/15) ha origine dalla decisione da parte di una società di comunicazioni svedese[558] di porre fine all'attività di conservazione dei dati e di cancellare quelli già registrati, a seguito dell'invalidazione della direttiva 2006/24/CE per effetto della sentenza *Digital Rights Ireland*. Dinanzi a tale presa di posizione, la *Post- och telestyrelesen,* autorità svedese di sorveglianza delle poste e delle telecomunicazioni, ha ordinato mediante ingiunzione alla *Tele2 Sverige AB* la conservazione dei dati di traffico e di ubicazione dei suoi abbonati. Secondo la normativa nazionale in materia di *data retention*[559], infatti, i fornitori di servizi di comunicazione elettronica erano tenuti a conservare, senza alcuna eccezione, il traffico di dati di ciascun utente, con riferimento a tutti mezzi di comunicazione elettronica.

Ritenendo tale obbligo di archiviazione generalizzato incompatibile con il *dictum* della Corte di Lussemburgo, la *Tele2 Sverige AB* si rivolgeva prima al Tribunale amministrativo di Stoccolma e poi alla Corte d'appello. In tale sede, i giudici nazionali hanno riscontrato una potenziale frizione della normativa in esame non solo rispetto al formante giurisprudenziale in materia ma anche all'articolo 15, paragrafo 1, della direttiva 2002/58/CE, decidendo di sospendere il procedimento in atto e di sottoporre la questione alla Corte di Giustizia.

---

[555] Il testo integrale dell'art. 15, par. 1, della direttiva 2002/58/CE è stato riportato *supra*.

[556] La direttiva sopracitata, c.d. *e-Privacy*, detta norme inerenti al «trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)». È stata modificata con la direttiva 2009/136/CE e si inserisce nell'ambito di un ampio intervento del legislatore comunitario che ha ritenuto opportuno garantire un livello omogeneo di tutela dei diritti fondamentali nel settore delle comunicazioni elettroniche.

[557] In prosieguo «Carta di Nizza» o semplicemente «Carta».

[558] Si tratta della *Tele2 Sverige AB* avente sede a Stoccolma. Per un maggiore approfondimento sull'operato di tale società si veda *www.tele2.com*.

[559] Si fa riferimento agli articoli da 16 a 16 f della LEK. Tale abbreviazione si riferisce alla *Lagen* (2003:389) *om elektronisk kommunikation*, legge sulle comunicazioni elettroniche. Siffatto testo normativo contiene norme sulla conservazione dei dati relativi alle comunicazioni elettroniche e la loro accessibilità da parte delle autorità nazionali.

Il secondo procedimento (C-698/15) ha origine con il ricorso[560] di alcuni cittadini inglesi[561] dinanzi all'Alta Corte di Giustizia avente ad oggetto l'articolo 1 del DRIPA[562], che consentiva al Ministro dell'interno di imporre ai *service providers*[563] la conservazione dei dati di traffico per la durata massima di un anno. Tale normativa veniva considerata in contrasto con i requisiti imperativi di diritto dell'Unione enunciati nella sentenza *Digital Rights Ireland* e applicabili alla legislazione interna in materia di conservazione di dati di traffico nonché di accesso a tali dati. Secondo la logica dei giudici nazionali, un atto interno dal contenuto identico rispetto a quello della direttiva 2006/24 non poteva che rivelarsi incompatibile rispetto agli articoli 7 e 8 della Carta di Nizza. Dinanzi a tale presa di posizione della Alta Corte di Giustizia, il Ministro dell'interno proponeva ricorso dinanzi alla Corte d'appello. In tale sede, i giudici nazionali sospendevano il procedimento *de quo* e sottoponeva il caso alla CGUE.

Nell'ambito delle cause riunite cui si è appena fatto cenno, due sono le principali questioni pregiudiziali sottoposte al vaglio della Corte di Lussemburgo.
Al centro di entrambe le questioni vi è l'incertezza in merito alle conseguenze della sentenza *Digital Rights Ireland* e alle implicazioni dell'annullamento della direttiva 2006/24/CE sulla legislazione interna.

9.2 La prima questione pregiudiziale.

La prima questione pregiudiziale, sollevata nella causa C-2013/15, ha ad oggetto il potenziale contrasto tra normativa svedese di *data retention* e l'articolo 15, paragrafo 1, della direttiva 2002/58. I giudici remittenti si sono domandati infatti se

[560] Il ricorso è stato presentato dinanzi alla *High Court of Justice* (*England & Wales*), *Queens' Bench Division* (*Divisional Court*), (Alta Corte di giustizia, sezione divisionale del Queens' Bench Regno Unito). Cfr. Corte giust. UE, Gr. Sez., sent. 21 dicembre 2016, cit., punto 52.
[561] Tale procedimento vede i signori *Tom Watson*, *Peter Brice* e *Geoffrey Lewis* contro il *Secretary of State for the Home Departmen*t, Ministro dell'Interno, Regno Unito di Gran Bretagna e Irlanda del Nord.
[562] La sigla di cui sopra è l'acronimo del *Data Retention and Investigatory Powers* Act 2014, legge sulla conservazione dei dati e sui poteri di indagine. L'articolo 1 dell'atto in esame, rubricato «Poteri in materia di conservazione dei dati relativi a comunicazioni rilevanti, con previsione di garanzie» prevede che il Ministro dell'Interno può imporre ad un fornitore di servizi la conservazione dei dati di trafficco mediante "avviso di conservazione". L'iniziativa deve risultare però necessaria e proporzionata rispetto ad una delle finalità previste dall'articolo 22, paragrafo 2, del *Regulation of Investigatory Powers Act 2000*, legge relativa poteri di indagine. Per consultare il DRIPA in lingua inglese si veda *www.legislation.gov.uk*.
[563] Per la definizione di *service providers* si rimanda al Cap. I.

l'art. 15[564] della direttiva 2002/58/CE, letto in combinato disposto con articoli 7, 8 e 52 della Carta*,* impedisca agli Stati membri di predisporre misure di «archiviazione generalizzata» dei dati di traffico.

Nel rispondere a tale quesito, la Corte ha verificato preliminarmente se una normativa nazionale quale quella in oggetto rientri nel campo di applicazione della direttiva e-*Privacy,* e più in generale nel diritto dell'Unione. Il dubbio era sorto a causa dell'articolo 1, paragrafo 3[565], della direttiva 2002/58/CE, che esclude dal proprio ambito le attività riguardanti la sicurezza pubblica, l'ordine pubblico e i settori che rientrano nel diritto penale. Nonostante i pareri discordanti dei governi intervenuti nel procedimento e della Commissione europea,[566] i giudici si sono pronunciati nel senso di ritenere le norme nazionali in questione ricomprese nel raggio di applicazione della direttiva 2002/58/CE. Una lettura in senso opposto, infatti, avrebbe delimitato eccessivamente la portata dell'atto di diritto derivato. [567]

Ciò posto, la Corte ha affermato che le disposizioni della direttiva e, in particolare, quanto sancito ai sensi dell'art. 5, paragrafo 1[568] si applicano a tutte le

---

[564] Per il testo dell'articolo si veda *supra*.

[565] L'art.1, paragrafo 3, della direttiva 2002/58/CE prevede che «La presente direttiva non si applica alle attività che esulano dal campo di applicazione del trattato che istituisce la Comunità europea, quali quelle disciplinate dai titoli V e VI del trattato sull'Unione europea né, comunque, alle attività riguardanti la sicurezza pubblica, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) o alle attività dello Stato in settori che rientrano nel diritto penale». In particolare, tale ultima espressione ha destato forti dubbi in merito all'ambito di applicazione della direttiva.

[566]Nel corso del procedimento, hanno presentato osservazioni scritte il Belgio, la Danimarca, l'Estonia, la Germania, l'Irlanda e l'Olanda, secondo i quali le normative nazionali in tema di *data retention* dovevano ritenersi incluse nel raggio di incidenza della direttiva 2002/48/CE. *A contrario*, la Repubblica Ceca affermava che le suddette disposizioni avessero come unico obiettivo la lotta contro la criminalità, ragion per cui dovessero escluse dalla portata applicativa dell'atto comunitario. Infine, il Regno Unito sosteneva vi rientrassero soltanto norme aventi ad oggetto l'archiviazione dei dati e non quelle riguardanti l'accessibilità agli stessi da parte delle autorità competenti. Come nota correttamente WOODS, se questa distinzione fosse stata accolta, avrebbe verosimilmente indotta ritenere inclusa nell'ambito di applicazione della direttiva soltanto l'attività di conservazione dei dati da parte dei fornitori di servizi. Tuttavia, la Corte non ha aderito a tale impostazione optando per una lettura dei due momenti della "conservazione" e dell'"accesso" come espressione di un atto complessivamente unitario. Sul punto, v. WOODS, *Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber),* in *www.eulawanalysis.blogspot.com*, 21 dicembre 2016.

[567] Sottolineano correttamente come la direttiva 2006/24/CE sia stata adottata nel 2006 proprio al fine di uniformare le disposizioni in materia di *data retention* in deroga al diritto alla *privacy* POLLICINO, BASSINI, *La Corte di Giustizia una trama ormai nota: la sentenza* Tele2 Sverige *sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, in *Dir. Pen. Cont.*, 2017.

[568] L'art.5, paragrafo 1, della direttiva 2002/58/CE prevede che «Gli Stati membri assicurano, mediante disposizioni di legge nazionali, la riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, nonché dei relativi dati sul traffico. In particolare, essi vietano l'ascolto, la captazione, la memorizzazione e altre forme di

misure di *data retention* adottate dagli Stati membri, indipendentemente dal fatto che la conservazione dei dati sia predisposta da enti privati o autorità statali. Ciò trova conferma nel considerando 21, che mira ad impedire l'accesso non autorizzato da parte di chiunque a «qualsiasi dato relativo [alle comunicazioni]»[569]. Pertanto, la Corte ha rilevato che anche la normativa inglese richiamata nella causa C-698/15 poteva essere ricompresa nell'ambito di applicazione della direttiva e-*Privacy*.

Una volta esaminato siffatto aspetto preliminare, la Corte è entrata nel merito della prima questione pregiudiziale verificando l'ammissibilità di un meccanismo di «archiviazione generalizzata». Nella linea argomentativa della Corte, si è ribadito, innanzitutto, che l'articolo 15[570] della direttiva 2002/58/CE rappresenta una deroga rispetto al principio fondamentale della riservatezza delle comunicazioni e, in quanto tale, debba essere oggetto di interpretazione restrittiva. Ciò posto, gli Stati membri non possono prevedere misure di conservazione dei dati per finalità diverse dalla «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». Secondo la CGUE, tale elenco ha, infatti, natura tassativa[571].

Di seguito, la Corte ha sottolineato l'esigenza di interpretare l'articolo 15 alla luce dei diritti fondamentali enunciati dalla Carta di Nizza. Infatti, soltanto mediante

---

intercettazione o di sorveglianza delle comunicazioni, e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza consenso di questi ultimi, eccetto quando sia autorizzato legalmente a norma dell'articolo 15, paragrafo 1. Questo paragrafo non impedisce la memorizzazione tecnica necessaria alla trasmissione della comunicazione fatto salvo il principio della riservatezza».

[569] Cfr. Corte giust. UE, Gr. Sez., 21 dicembre 2016, *Tele2 Sverige*, cit., punto 77.

[570] Al fine di una maggiore comprensione della sentenza in esame, si ritiene utile riportare l'articolo 15, paragrafo 1, della direttiva 2002/58 nella sua interezza: «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/CE, una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioé 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 comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea». L'articolo *de quo,* rubricato «Applicazione di alcune disposizioni della direttiva 95/46/CE», va ad attuare le disposizioni della direttiva citata relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Tale atto è stato abrogato il 27 aprile 2016 con l'approvazione del Regolamento generale sulla protezione dei dati 2016/679. Per visionare il testo della direttiva ormai non più in vigore si veda *www.eur-lex.europa.eu.*

[571] Cfr. Corte giust. UE, Gr. Sez., sent. 21 dicembre 2016, *Tele2 Sverige,* cit., punto 90.

una lettura "costituzionalmente orientata" dell'articolo in esame è possibile capire se la normativa di diritto interno contrasti con i principi contenuti nella Carta di Nizza.

Innanzitutto, ai sensi dell'articolo 52, paragrafo 1, ogni limitazione all'esercizio dei diritti e delle libertà deve rispettare il «contenuto essenziale» di questi ultimi e rispondere al principio di proporzionalità. Tale criterio, non solo discende dalla consolidata giurisprudenza della Corte, secondo cui le restrizioni al rispetto della vita privata devono intervenire nei limiti dello «stretto necessario»[572], ma è confermata dalla frase di apertura dell'articolo 15 della direttiva 2002/58/CE. La norma citata prevede che gli Stati membri possono imporre una misura in deroga al principio di riservatezza delle comunicazioni soltanto se «necessaria, opportuna e proporzionata all'interno di una società democratica». Ciò è confermato dal considerando 11[573], secondo cui la suddetta eccezione deve essere «strettamente» proporzionata allo scopo perseguito dall'atto.

Nel verificare se la normativa svedese in questione, soddisfi i requisiti anzidetti la Corte ha condotto una valutazione accurata. I giudici hanno rilevato che la disciplina nazionale prevede una conservazione generalizzata sistematica di tutti i dati relativi al traffico e all'ubicazione rievocando quasi *in toto* il contenuto della direttiva 2006/24/CE, ormai abrogata. Per evitare che attraverso una norma di diritto in interno si realizzi un "tentativo di elusione"[574] di quanto affermato nella sentenza *Digital Rights*, la Corte ha riproposto lo stesso *iter* argomentativo.

---

[572] Cfr. Corte giust. UE, Gr. Sez., sent. 21 dicembre 2016, *Tele2 Sverige,* cit., punto 96.

[573] Il considerando 11 dispone che «La presente direttiva, analogamente alla direttiva 95/46/ CE, non affronta le questioni relative alla tutela dei diritti e delle libertà fondamentali inerenti ad attività che non sono disciplinate dal diritto comunitario. Lascia pertanto inalterato l'equilibrio esistente tra il diritto dei cittadini alla vita privata e la possibilità per gli Stati membri di prendere i provvedimenti di cui all'articolo 15, paragrafo 1, della presente direttiva, necessari per tutelare la sicurezza pubblica, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) e l'applicazione della legge penale. Di conseguenza la presente direttiva non pregiudica la facoltà degli Stati membri di effettuare intercettazioni legali di comunicazioni elettroniche o di prendere altre misure, se necessario, per ciascuno di tali scopi e conformemente alla Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali, come interpretata dalle sentenze della Corte europea dei diritti dell'uomo. Tali misure devono essere appropriate, strettamente proporzionate allo scopo perseguito, necessarie in una società democratica ed essere soggette ad idonee garanzie conformemente alla precitata Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali».

[574] L'espressione è di POLLICINO, BASSINI, *La Corte di Giustizia una trama ormai nota: la sentenza* Tele2 Sverige *sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, in *Dir. Pen. Cont.*, 2017, 6.

Innanzitutto, si è ribadito che l'attività di archiviazione di dati di traffico realizza di per sé una ingerenza di vasta portata sul diritto alla *privacy,* che la giurisprudenza giudica particolarmente grave[575]. Una simile interferenza sui diritti fondamentali può risultare legittima soltanto in presenza di un interesse generale dell'Unione europea altrettanto importante, quale l'accertamento e la persecuzione di reati gravi. Nonostante l'efficacia della lotta contro la criminalità grave[576] dipenda, in parte, dalla disponibilità di moderne tecniche di indagine, un simile obiettivo, per quanto fondamentale, non giustifica di per sé una conservazione automatica e generalizzata dei dati di traffico[577].

Al contrario, l'impianto normativo istituito dalla direttiva 2002/58/CE esige che l'archiviazione dei dati rappresenti l'eccezione in un sistema che, in linea di massima, privilegi la riservatezza delle comunicazioni. In tal senso, una normativa interna che preveda una archiviazione dei dati estesi alla totalità delle persone che utilizzano mezzi di comunicazione elettronica, senza che queste risultino, anche solo indirettamente, collegate ad un'azione penale in corso, eccede i limiti dello «stretto necessario» e non può trovare fondamento nell'articolo 15 della direttiva e-*Privacy*.

Una volta rilevata l'incompatibilità di entrambe le normative nazionali rispetto all'articolo 15, paragrafo 1, della direttiva 2002/58/CE, letto alla luce degli articoli 7, 8 e 52[578] della Carta di Nizza, la Corte ha stilato un elenco di requisiti che il legislatore nazionale è tenuto a rispettare nel predisporre misure di *data retention*[579].

Secondo i giudici, in primo luogo, occorre prevedere in modo chiaro e preciso le condizioni secondo cui le autorità competenti possono procedere, a titolo preventivo, alla conservazione dei dati. Mediante la predeterminazione di una serie di requisiti sostanziali, si garantisce agli utenti i cui dati sono stati conservati di disporre di tutele sufficienti a proteggere le loro informazioni personali contro rischi di abuso.

---

[575] Cfr. Corte giust. UE, Gr. Sez., 21 dicembre 2016, *Tele2 Sverige,* cit., punto 100.
[576] Evidenzia come la Corte faccia riferimento soltanto alla criminalità grave, mentre l'articolo 15 della direttiva 2002/58/CE faccia riferimento, in termini più ampi alla prevenzione a all'accertamento di attività criminose in genere WOODS, *Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber), cit., 2*.
[577] Si veda, per analogia, in merito alla direttiva 2006/24/CE, Corte giust. UE, Gr. Sez., 8 aprile 2014, *Digital Rights Ireland*, cit., punto 51.
[578]Si ricorda qui che i criteri secondo i quali è possibile una limitazione dei diritti e delle libertà fondamentali ai sensi dell'articolo 52 della Carta di Nizza sono: una previsione di legge; il rispetto del contenuto essenziale dei diritti individuali convolti; il perseguimento di un obiettivo di interesse generale e il rispetto del principio di proporzionalità.
[579] Cfr. Corte giust. UE, Gr. Sez., sent. 21 dicembre 2016, *Tele2 Sverige,* cit., punto 109.

In secondo luogo, la Corte ha affermato che l'attività di conservazione deve sempre essere finalizzata all'accertamento e al perseguimento dei reati gravi. In particolare, è necessario che il legislatore istituisca un nesso, almeno indiretto, tra i dati da conservare e il reato per cui si procede.

Da ultimo, la Corte ha sottolineato la necessità di adoperare cautele analoghe nella determinazione dei potenziali destinatari dell'operazione di archiviazione, ad esempio, mediante l'utilizzo di un criterio geografico che individui macro-aree in cui si riscontri un elevato rischio di preparazione o di commissione di reati.

9.3 Segue: la seconda questione pregiudiziale.

La seconda questione pregiudiziale della causa C-203/15, analoga alla prima questione sollevata nella causa C-698/15, rappresenta il naturale corollario di quanto affermato sul punto precedente[580]. Mediante tale quesito, i giudici nazionali hanno chiesto alla Corte se l'articolo 15 sopracitato impedisca agli Stati membri di prevedere l'accesso ai dati personali da parte delle autorità inquirenti senza il previo controllo da parte di un'autorità giurisdizionale. Nell'ordinamento inglese, infatti, si riconosceva al Ministro dell'interno il potere di imporre ai fornitori di servizi l'archiviazione dei dati personali senza alcuna autorizzazione preventiva da parte di giudici[581].

Nella risoluzione di tale secondo punto, la Corte ha ribadito il principio di proporzionalità e di necessità secondo cui il legislatore nazionale è tenuto a prevedere *ex ante* i requisiti sostanziali e procedurali per cui è possibile acquisire i dati da parte delle autorità competenti. Al fine di assicurare il rispetto di tali condizioni, la legittimità della richiesta di acquisizione deve essere subordinata ad un controllo effettuato da un giudice o da un'entità amministrativa indipendente, salvo casi di particolare urgenza[582].

Inoltre, la Corte ha sottolineato la necessità che le autorità competenti cui è consentita la conoscibilità dei dati di traffico diano notizia alle persone interessate

[580] Prima di entrare nel merito della questione, i giudici osservavano in via preliminare che la Corte d'appello amministrativa di Stoccolma aveva chiesto di rispondere a tale quesito soltanto nell'ipotesi in cui si fosse data risposta negativa al primo. Tuttavia, avendo rilevato che tale seconda questione risultasse indipendente rispetto al carattere generalizzato dell'attività di conservazione, la Corte decideva di rispondere in ogni caso a tale interrogativo. Si veda in tal senso Corte giust. UE, Gr. Sez., sent. 21 dicembre 2016, *Tele2 Sverige*, cit., punto 113.
[581] Cfr. Corte giust. UE, Gr. Sez., 21 dicembre 2016, *Tele2 Sverige,* cit., punto 114.
[582] In analogia, si veda la sentenza Corte giust. UE, Gr. Sez., 18 aprile 2014, *Digital Rights Ireland*, cit., punto 62.

dell'avvenuta acquisizione[583]. A partire dal momento in cui tale comunicazione non è in grado di compromettere l'esito delle indagini per cui si procede, essa costituisce, invece, un passaggio fondamentale per assicurare il diritto di ricorso ai sensi dell'articolo 15, paragrafo 2[584], della direttiva 2002/58/CE.

Da ultimo, si è affermato che, ai sensi dell'articolo 4, paragrafi 1 e 1-*bis*[585]della direttiva *e-Privacy*, i fornitori dei servizi di comunicazioni sono tenuti ad adottare misure di sicurezza idonee a garantire i dati contro il rischio di accesso illecito. In particolare, gli Stati membri devono istituire un'autorità indipendente che garantisca il rispetto di uno *standard* minimo di tutela delle persone fisiche riguardo ai dati personali. Secondo i giudici, tale controllo, previsto espressamente dall'articolo 8, paragrafo 3[586], della Carta di Nizza costituisce elemento fondante del diritto al rispetto dei dati personali[587].

Sulla base delle considerazioni sopra enucleate, la Corte di Giustizia ha accolto la seconda questione della causa C-203/15 e la prima della causa C-698/15. In tal senso, ha dichiarato che l'articolo 15, paragrafo 1 della direttiva 2002/58/CE, interpretato ai sensi degli articoli 7, 8 e 11 nonchè dell'articolo 52 della Carta di Nizza, è in contrasto con «una normativa nazionale la quale disciplini la protezione e la sicurezza dei dati relativi al traffico e dei dati relativi all'ubicazione, e segnatamente

---

[583] Cfr. Corte giust. UE, Gr. Sez., 21 dicembre 2016, *Tele2 Sverige*, cit., punto 121.

[584] Le disposizioni del capo III della direttiva 95/46/CE relative ai ricorsi giurisdizionali, alle responsabilità e alle sanzioni si applicavano relativamente alle disposizioni nazionali adottate in base alla presente direttiva e con riguardo ai diritti individuali risultanti dalla stessa.

[585] L'articolo 4 della direttiva 2002/58, modificato dalla direttiva 2009/136/CE, è ora rubricato «Sicurezza del trattamento». Ai paragrafi 1 e 1 *bis* sopracitati dispone che «Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico deve prendere appropriate misure tecniche e organizzative per salvaguardare la sicurezza dei suoi servizi, se necessario congiuntamente con il fornitore della rete pubblica di comunicazione per quanto riguarda la sicurezza della rete. Tenuto conto delle attuali conoscenze in materia e dei loro costi di realizzazione, dette misure assicurano un livello di sicurezza adeguato al rischio esistente.

1. Fatta salva la direttiva 95/46/CE, le misure di cui al paragrafo 1 quanto meno:

— garantiscono che i dati personali siano accessibili soltanto al personale autorizzato per fini legalmente autorizzati,

— tutelano i dati personali archiviati o trasmessi dalla distruzione accidentale o illecita, da perdita o alterazione accidentale e da archiviazione, trattamento, accesso o divulgazione non autorizzati o illeciti,

— garantiscono l'attuazione di una politica di sicurezza in ordine al trattamento dei dati personali.

Le autorità nazionali competenti sono legittimate a verificare le misure adottate dai fornitori di servizi di comunicazione elettronica accessibili al pubblico e a emanare raccomandazioni sulle migliori prassi in materia di sicurezza che tali misure dovrebbero conseguire».

[586] L'articolo 8 della Carta di Nizza, dopo aver enunciato il principio della protezione dei dati di carattere personale prevede che «Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

[587] In analogia si veda sentenza *Digital Rights* Corte giust. UE, Gr. Sez., sent. 8 aprile 2014, *cit.*, punto 68.

l'accesso delle autorità nazionali competenti ai dati conservati, senza limitare, nell'ambito della lotta contro la criminalità, tale accesso alle sole finalità di lotta contro la criminalità grave, senza sottoporre detto accesso ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente, e senza esigere che i dati di cui trattasi siano conservati nel territorio dell'Unione»[588].

Infine, la Corte dichiarava la propria incompetenza a pronunciarsi direttamente sulla validità delle norme nazionali richiamate nei procedimenti principali. Incombe, dunque, sui giudici del rinvio stabilire se e in quale misura le normative interne in tema di *data retention* rispettino le condizioni ai sensi dell'articolo 15 della direttiva e-*Privacy,* così come interpretato dalla giurisprudenza della Corte.

Mediante la sentenza in commento la Corte ha realizzato il necessario completamento del percorso avviato con la caducazione della direttiva 2006/24/CE. Mentre nella sentenza *Digital Rights Ireland* si è analizzata la compatibilità un atto di diritto derivato rispetto alla Carta dei diritti dell'Unione, con questa pronuncia si è definita la competenza ermeneutica della Corte rispetto alle fonti nazionali. Nel primo caso la CGUE è risultata detentrice di un "monopolio interpretativo" in base al quale può disporre l'annullamento di atti di diritto derivato se ritenuti incompatibili rispetto ai principi espressi dai Trattati, nel secondo caso ha un potere di incidenza ridotto[589].

Nella sentenza *Tele2 Sverige*, infatti, la Corte si è limitata a fornire i parametri in base ai quali i giudici nazionali debbano valutare la legittimità delle norme di diritto interno in materia *data retention*, rimettendo ai tribunali nazionali il compito di dichiarare l'eventuale illegittimità degli atti, nonché al legislatore nazionale di abrogare le norme considerate in contrasto con l'impianto comunitario[590].

In tal modo, la Corte ha sgomberato il campo relativamente alle incertezze residue sulla sussistenza di un collegamento tra le normative nazionali in materia di *data retention*, soprattutto tra quelle che non derivassero direttamente dalla trasposizione della direttiva 2006/24/CE, e il diritto dell'Unione. Allo stesso tempo, ha, però, riconosciuto i limiti del suo potere di azione rispetto all'interpretazione

[588] Cfr. Corte giust. UE, Gr. Sez., sent. 21 dicembre 2016, *cit.*, punto 125.
[589] Cfr. FLOR, *La Corte di giustizia considera la direttiva europea 2006/24 sulla cd*. "data retention" *contraria ai diritti fondamentali. Una lunga storia a lieto fine?* in *Dir. Pen. contemp., 2014*, fasc. 2, 178.
[590] In tal senso v. CAGGIANO, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione, cit.*, 68.

pregiudiziale delle fonti di diritto interno, rimarcando la necessità di garantire un dialogo tra i tribunali nazionali e la Corte di giustizia in un'ottica di cooperazione giudiziaria.

Inoltre, per quanto riguarda la *vexata quaestio* circa l'esigenza di trovare un equilibrio tra le ragioni di pubblica sicurezza e la tutela della riservatezza delle comunicazioni, il giudice dell'Unione si è definitivamente pronunciato a favore delle seconde. Nel fornire un'interpretazione della direttiva 2002/58/CE, e in specie alla deroga prevista dall'art. 15 alla protezione della *privacy* digitale, si è optato ancora una volta per una "rilettura" costituzionalmente orientata o quanto meno *human rights oriented*[591] delle normative preesistenti al Trattato di Lisbona.

In materia di conservazione dei dati di traffico, si è, dunque, definitivamente realizzato l'abbandono definitivo del precedente approccio secondo cui si sacrificava la tutela dei diritti fondamentali nella lotta al terrorismo internazionale[592], mediante una legislazione di tipo emergenziale e altamente invasiva nei diritti degli utenti. Tale risultato si è ottenuto mediante due passaggi: da una parte vincolando le istituzioni europee al rispetto della *privacy* digitale (*Digital Rights Ireland*) e dall'altra, i legislatori degli Stati membri (*Tele2 Sverige AB*). Infine, si è consolidato un approdo evolutivo che vede la proclamazione di *standard* di tutela elevati al fine di tutelare i diritti fondamentali incisi dalla *data retention*.

10. Il caso *H.K. Danmark* (2021).

Dopo le sentenze *Digital Rights Ireland* e *Tele2 Sverige AB*, i giudici di Lussemburgo sono intervenuti in più occasioni in materia di acquisizione dei dati di traffico. In tal senso, è opportuno fare riferimento alle sentenze *Privacy international*[593] e *La Quadrature du Net*[594], tramite le quali la Corte di Giustizia ha nuovamente ribadito che il principio di proporzionalità osta ad una normativa interna secondo cui si dispone una raccolta generalizzata e indiscriminata dei dati di traffico. Inoltre, si è chiarito ulteriormente che le legislazioni nazionali in materia di *data*

[591] L'espressione è di POLLICINO, BASSINI, *La Corte di Giustizia una trama ormai nota: la sentenza* Tele2 Sverige *sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, *cit.*, 4.
[592] Tale approccio emergenziale è rinvenibile nella direttiva 2006/24/CE in cui l'attacco terroristico di Londra è esplicitamente nel Considerando 10.
[593] Cfr. Corte giust. UE, sent. 6 ottobre 2020, *La Quadrature du Net (*Cause riunite C-511/18, C-512/18 e C-520/18), in *www.curia.europa.eu*.
[594]Cfr. Corte giust. UE, sent. 6 ottobre 2020, *Privacy International*, in *www.curia.europa.eu.*

retention rientrano pienamente nell'ambito di applicazione della direttiva 2002/58/CE, anche se la conservazione dei dati avviene per finalità di sicurezza nazionale. Neppure queste ultime possono, infatti, giustificare disposizioni nazionali che consentano la trasmissione generalizzata di dati ai servizi di *intelligence* e di sicurezza.

Da ultimo, è da segnalare la recentissima sentenza del 2 marzo 2021[595], con cui la Corte di Giustizia ha aggiunto un nuovo *step* alla parabola evolutiva segnata in materia di *data retention*. Nel caso di specie[596], la controversia tra origine dalla domanda di rinvio pregiudiziale *ex* art. 267 TFUE[597] da parte della *Riigikohus* (Corte suprema estone) contro l'imputata H.K., condannata alla pena detentiva di due anni per furto e per aver compiuto atti di contro le persone coinvolte nel procedimento penale a suo carico[598]. La sentenza di condanna del Tribunale di primo grado estone si basava, tra gli elementi di prova a carico dell'imputata, sui tabulati relativi ai dati di traffico telefonico acquisiti dall'autorità inquirente presso il gestore dei servizi di telecomunicazione[599]. Avverso la stessa è stato proposto appello e, successivamente, ricorso dinanzi alla Corte Suprema, in cui l'imputata ha eccepito l'inammissibilità dell'attività di acquisizione dei dati per contrasto della normativa nazionale rispetto all'art. 15, paragrafo 1, della direttiva 2002/58/CE[600] del Parlamento europeo e del Consiglio Ue, così come interpretato alla luce degli artt. 7, 8 e 11, nonché dell'art. 52, paragrafo 1, della Carta di Nizza.

Dinanzi a siffatta eccezione di parte, il *Riigikohus* ha ritenuto opportuno sospendere il procedimento in corso e sottoporre ai giudici di Lussemburgo tre questioni pregiudiziali. In primo luogo, [601] si è chiesto se l'art. 15, paragrafo 1 della direttiva 2002/58/CE debba essere interpretato nel senso che l'accesso ai dati di traffico da parte delle autorità nazionali debba essere limitato alle forme di criminalità

[595] Corte giust. UE, Gr. Sez., sent. 2 marzo 2021, *H.K. Danmark,* in *www.curia.europa.eu.*
[596] Sul punto v. RINALDINI, 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 *www.giurisprudenzapenale.com.*
[597] Per un approfondimento sul rinvio pregiudiziale si rimanda a quanto detto *supra.*
[598] Cfr. Corte giust. UE, Gr. Sez., sent. 2 marzo 2021, *H.K. Danmark,* cit., punto 20.
[599] Nella sentenza, si precisa che i dati di traffico acquisiti erano relativi ad utenze intestate o utilizzate da H.K. e a diversi codici internazionali di identificazione di apparecchiatura telefonica mobile, riferiti a vari periodi fra il 2015 e il 2016.
[600] Per il contenuto dell'art. 15 della direttiva 2002/58/CE si veda quanto detto *supra*.
[601] Cfr. Corte giust. UE, Gr. Sez., sent. 2 marzo 2021, *H.K. Danmark,* cit., punto 21.

grave[602], in quanto trattasi di attività che costituisce un'ingerenza grave nei diritti fondamentali tutelati dagli artt. 7, 8 e 11 della Carta di Nizza. In secondo luogo, si è sottoposta alla CGUE la questione circa la quantità di dati di cui ordinamento nazionale può disporre l'acquisizione senza incorrere nella violazione del principio di proporzionalità ai sensi dell'art. 52 della Carta di Nizza[603]. Da ultimo, la Corte suprema estone ha chiesto se la normativa nazionale relativa alla *data retention* possa attribuire al Pubblico Ministero, organo che dirige l'attività di indagine e di istruttoria penale, il potere di acquisire i tabulati relativi al traffico telefonico e telematico, senza il controllo preventivo di un giudice o di un'autorità indipendente. In sintesi, con tale ultima questione, i giudici estoni hanno messo in dubbio che il P.M., organo della pubblica accusa, possa essere dotato dei requisiti di indipendenza e di terzietà richiesti dall'ordinamento comunitario per la predisposizione di una misura che, di fatto, risulta assimilabile ad un mezzo di ricerca della prova.

In risposta a suddette questioni pregiudiziali, è intervenuta la Corte di giustizia che, enunciando principi innovativi, ha aggiunto un *quid pluris* rispetto a quanto già affermato dalla giurisprudenza comunitaria nelle sentenze *Digital Rights Ireland* e *Tele2 Sverige*. Di seguito, si ripercorreranno i nodi essenziali della pronuncia in esame.

In primis, la Corte ha esaminato congiuntamente le prime due questioni pregiudiziali[604]. A tal proposito, ha, dapprima, ribadito che l'art. 15, paragrafo 1, interpretato in conformità agli artt. 7, 8 e 11 della Carta osta a normative nazionali che prevedono la conservazione «generalizzata» e «indifferenziata dei dati relativi al traffico per finalità di prevenzione e di accertamento dei reati»[605]. Inoltre, i giudici hanno affermato che, in base al principio di proporzionalità, soltanto l'obiettivo di interesse generale di reprimere le forme gravi di criminalità è idoneo a giustificare

[602] La questione è stata sottoposta ancora una volta alla Corte dopo che con la pronuncia del 2 ottobre 2018, nel caso *Ministerio Fiscal*, si era fatto un fatto un piccolo passo indietro, riconoscendo la possibilità agli Stati membri di predisporre la *data retention* anche per reati non gravi. In questa sede, è stata ritenuta possibile la conservazione dei dati di traffico telefonico e telematico, qualora le ingerenze nella "sfera privata" del singolo da parte della pubblica autorità non siano da considerarsi gravi. A tale proposito, la Corte ha quindi specificato che l'acquisizione di dati idonei ad identificare il titolare di carte SIM, attivate con codice IMEI, di un telefono cellulare rubato, fosse possibile a prescindere dalla finalità di accertare di un reato grave, in quanto la ricerca dei soli dati anagrafici non sarebbe di per sé sola idonea a ledere i diritti dell'individuo. Cfr. Corte giust. UE, sent. 2 ottobre 2018, *Ministerio Fiscal*, *cit*., punto 54.

[603] Cfr. Corte giust. UE, Gr. Sez., sent. 2 marzo 2021, *H.K. Danmark,* cit., punto 22.

[604] Cfr. Corte giust. UE, Gr. Sez., sent. 2 marzo 2021, *H.K. Danmark,* (C-746/18), punto 27.

[605] In analogia, v. anche Corte giust. UE, sent. del 6 ottobre 2020, *La Quadrature du Net* e a., cit., punto 168.

«gravi ingerenze» rispetto alla "sfera privata" dell'individuo, come quelle realizzate dall'attività di conservazione dei dati di traffico. Pertanto, qualora la normativa nazionale, come quella estone in discussione nel procedimento *de quo*, non limiti la *data retention* a finalità di accertamento e perseguimento dei gravi, allora questa risulta conforme al principio di proporzionalità soltanto laddove non realizzi interferenze gravi rispetto ai diritti fondamentali sopracitati.

Ciò avviene soltanto quando i dati di traffico archiviati non permettano, di per sé soli, «di conoscere la data, l'ora, la durata e i destinatari delle comunicazioni effettuate, né i luoghi in cui tali comunicazioni sono avvenute o la frequenza delle stesse con determinate persone nel corso di un dato periodo»[606]. *A contrario*, qualora da tali informazioni si possa dedurre sia il mezzo di comunicazione adoperato dall'utente e sia le coordinate spaziali e temporali delle apparecchiature terminali da quest'ultimo utilizzate, così da trarre «precise conclusioni sulla vita privata dell'individuo», allora l'ingerenza causata dall'acquisizione di tali dati non può non ritenersi «grave». Ciò indipendente dalla durata del periodo di archiviazione dei dati siffatti e dalla quantità informazioni raccolte. Pertanto, in siffatti casi, l'attività di acquisizione e conservazione dei dati "esterni" alla comunicazione deve essere limitata allo «stretto necessario» e, dunque, circoscritta ad una categoria di reati considerati gravi.

Alla luce delle considerazioni che precedono, la Corte di Giustizia ha risposto alla prima e alla seconda questione pregiudiziale sollevata nel procedimento *de quo* affermando che l'articolo 15, paragrafo 1, della direttiva 2002/58, interpretato alla luce degli articoli 7, 8 e 11 della Carta, debba essere letto nel senso che esso osta ad una legge nazionale, che consenta all'autorità pubblica di accedere ad una archiviazione generalizzata di dati traffico, senza che tale accesso sia limitato all'accertamento reati gravi[607].

Di seguito, i Giudici di Lussemburgo si sono pronunciati in merito al terzo quesito del giudice del rinvio circa l'idoneità del pubblico ministero a predisporre l'acquisizione dei tabulati telefonici e telematici senza il vaglio di merito di un giudice o di un'autorità indipendente. Sul punto, si è precisato che, nonostante spetti agli Stati

[606] Cfr. Corte giust. UE, Gr. Sez., sent. 2 marzo 2021, *H.K. Danmark, cit.*, punto 53.
[607] Cfr. Corte giust. UE, Gr. Sez., sent. 2 marzo 2021, *H.K. Danmark, cit.*, punto 53.

membri stabilire le condizioni sostanziali e procedurali in base alle quali le autorità nazionali possono disporre dell'acquisizione dei dati di traffico, essi devono adeguarsi a requisiti minimi stabilità in ambito comunitario in base al principio di proporzionalità. Pertanto, in tale sede, la Corte ha ribadito che una normativa interna che consenta alle pubbliche autorità di accedere a tutti i dati conservati, indipendentemente dalla sussistenza di un collegamento, almeno indiretto, rispetto al reato per cui si procede, non può considerarsi circoscritta allo stretto necessario. Ne consegue che la normativa nazionale in materia di *data retention* deve prevedere requisiti oggettivi che definiscano circostanze in base alle quali è consentito alle autorità nazionali accedere ai dati in questione.

Inoltre, i giudici di Lussemburgo hanno affermato che, al fine di assicurare il rispetto di tali condizioni, è necessario che l'acquisizione dei dati sia subordinata al preventivo controllo di un giudice o di un'autorità amministrativa indipendente che assicuri «conciliazione dei diversi interessi e diritti in gioco». Secondo la Corte, l'autorità giurisdizionale è, infatti, preposta ad assicurare «il giusto equilibrio tra, da un lato, gli interessi connessi alle necessità dell'indagine nell'ambito della lotta contro la criminalità e, dall'altro, i diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali delle persone i cui dati sono interessati dall'accesso». In aggiunta, si è affermato che l'attività di controllo deve essere svolta «in modo obiettivo e imparziale» da un organo che goda di uno *status* di indipendenza e sia in grado agire svincolato da qualsiasi «influenza esterna». L'autorità incaricata di svolgere il controllo preventivo sull'attività di acquisizione dei dati di traffico coincide, dunque, necessariamente con il giudice o con un'autorità amministrativa indipendente[608].

Al contrario, la Corte di Giustizia ha affermato che il pubblico ministero non è in grado di effettuare il suddetto vaglio di legittimità dell'attività acquisitiva in oggetto. In quanto a capo dell'indagine penale, l'autorità inquirente risulta, infatti, priva della posizione di neutralità nei confronti delle parti coinvolte all'interno del procedimento penale e mancante del c.d. *status* di terzietà. Alla luce di tali circostanze, i giudici di Lussemburgo hanno dichiarato che l'articolo 15, paragrafo 1, della direttiva

[608] Cfr. RINALDINI, 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*, 2021, in *www.giurisprudenzapenale.it.*

2002/58/CE, deve essere interpretato nel senso che osta ad una normativa nazionale, la quale attribuisca al pubblico ministero, e non ad un giudice o ad una autorità amministrativa indipendente, il compito autorizzare l'accesso ai dati relativi al traffico[609].

Nel capitolo successivo, si valuterà il forte impatto che tali principi di diritto della Corte di Giustizia Ue sono in grado di produrre nell'ordinamento normativo italiana, in cui compete proprio al pubblico ministero predisporre l'acquisizione dei dati "esterni" alla comunicazione, in assenza di vaglio preventivo del giudice.

[609] Cfr. Corte giust. UE, Gr. Sez., sent. 2 marzo 2021, *H.K. Danmark, cit.*, punto 59.

CAPITOLO III

PROFILI DI CRITICITÀ DELLA DISCIPLINA ITALIANA IN MATERIA DI *DATA RETENTION*

SEZIONE I

Distonie tra l'art. 132 del Codice *Privacy* e il diritto Ue

1. Note introduttive.

Nel capitolo precedente, si è cercato di dare prova della marcata attitudine della c.d. *data retention* ad aggredire non solo l'apparato assiologico della Costituzione[610] ma anche il quadro delle fonti internazionalistiche in materia di diritti fondamentali dell'individuo. Si è dimostrato che siffatto strumento di acquisizione probatoria sia idoneo ad interferire sia con le tradizionali "libertà negative" (artt. 14[611] e 15[612] Cost.) sia con la tutela della "sfera privata" del singolo (7 CDFUE)[613] e con il diritto di ciascuno a mantenere il controllo sui propri dati personali (8 CDFUE)[614].

Se da una parte, la giurisprudenza italiana si è dimostrata incline a sottovalutare la capacità intrusiva dell'attività di conservazione dei dati "esteriori" alle comunicazioni, evidenziandone la differenza rispetto ad altri strumenti di indagine[615]; dall'altra, presso la Corte di Giustizia, la c.d. *data retention* è stata protagonista di una parabola "ascendente"[616] durante la quale si è assistito al progressivo "disvelamento" dei valori costituzionali coinvolti. Partendo dall'assunto secondo cui la protezione dei

---

[610] L'espressione è di SILVESTRI, *L'individuazione dei diritti della persona*, in *Dir. pen. Cont.*, 2018, 1.
[611] Sul punto si veda Cap II § 3.
[612] Cfr. Cap. II § 2.
[613] Cfr. Cap II § 6.
[614] Per l'esegesi dell'art. 8 della Carta di Nizza si rimanda II § 7.
[615] In particolare, si fa riferimento alle celebri sentenze della Corte costituzionale del 6 aprile 1973, n. 34, in *Giur. cost.*, 1973, 316 e alla sent. 11 marzo 1993, n. 81, in *www.cortecostituzionale.it.* In quest'ultima pronuncia, i Giudici di legittimità, hanno affermato che l'istituto della *data retention* realizzi una un'interferenza "attenuata" del diritto fondamentale tutelato dall'art. 15 Cost. rispetto ad altre metodologie di indagine tra cui le intercettazioni. Per un approfondimento sul contenuto della pronuncia v. Cap II § 2.
[616] L'espressione è di MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen*., 2015, 784. In termini analoghi, LUPÀRIA, Data retention *e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, in *Dir. internet,* 2019, 4, 760.

dati è – ormai da tempo[617] – una materia di piena competenza dell'Unione europea[618], i giudici di Lussemburgo hanno affermato che siffatto valore, rientrante nel più ampio bene giuridico della «riservatezza», debba essere oggetto di tutela particolarmente intensa.

Di conseguenza, il legislatore che adotti misure in deroga agli art. 7 e 8 della Carta di Nizza, è tenuto al rispetto del principio di proporzionalità[619], ovvero del minor sacrificio possibile del bene medesimo[620]. Sul piano applicativo, siffatto canone rappresenta un "criterio di razionalità pratica" in base al quale verificare la legittimità dell'interferenza realizzata dallo Stato nella "sfera privata" del singolo. Al fine di evitare ingiustificate compressioni del diritto fondamentale, l'autorità di *law enforcement* che predisponga una misura restrittiva è, dunque, tenuta a verificarne la ragionevolezza rispetto alle esigenze del caso concreto, secondo i parametri della idoneità e della "stretta necessità", dandone, poi, conto, mediante atto motivato[621].

Mediante l'individuazione di siffatti *standard* di tutela, la Corte[622] ha indicato al legislatore europeo, la soluzione per garantire i diritti inviolabili dell'individuo, senza dover rinunciare *in toto* agli strumenti tecnologici indispensabili[623] per la prevenzione e l'accertamento di gravi reati, *sub specie* alla *data retention*[624]. Proprio a livello sovranazionale, si è assistito, dunque, ad un mutamento culturale che ha visto l'individuazione di un nuovo equilibrio tra *auctoritas* e *libertas,* da raggiungere

---

[617] Si faccia riferimento alla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, «relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati», che aveva portato il legislatore interno ad emanare le note leggi n. 675 e 676 del 1996. Per un approfondimento sul quadro normativo in materia di protezione dei dati personali v. Cap. II § 7.

[618] Sul punto v. MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale*, *cit.*, 776. L'Autore sottolinea che si tratti di una competenza strumentale a garantire il buon funzionamento del mercato interno.

[619] Sul canone di proporzionalità, sulla sua genesi nell'ordinamento tedesco e sulla sua affermazione come principio riformatore dei rapporti tra diritto europeo e nazionale si veda GALETTA, *Il principio di proporzionalità fra. Diritto nazionale e diritto europeo (con uno sguardo anche al di là dei confini dell'Unione Europea)*, in *Riv. It. Dir. pubbl. comun*., 2019, 927 e ss.

[620] È possibile ricavare il principio di proporzionalità anche dall'art. 8, par. 2, CEDU, contenente anch'esso una simile clausola generale.

[621] Sul punto v. ANDOLINA, *L'ammissibilità degli strumenti di captazione dei dati personali tra standard di tutela della* privacy *e onde eversive*, in *Arch. pen.*, 2015, n. 3, 936.

[622] Si fa riferimento alle sentenze della Corte di Giustizia *Digital Rights Ireland*, *Tele2 Sverige AB* e *H.K. Danmark* ampiamente approfondite nel Cap. II, a cui si rinvia.

[623] Sull'irrinunciabilità della tecnologia nel processo penale si veda, *ex multis*, MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale*, *cit.*, 788.

[624] In tal senso, PASCALI, *La* data retention *dopo la dichiarazione di invalidità della Direttiva 2006/24/CE*, in *Riv. elettronica dir. econ. Manegement*, 2015, 3, 87. IOVENE, Data retention *tra passato e futuro. Ma quale presente?* in *Cass. Pen*., 2014, 4274.

ogniqualvolta che l'autorità statale entri in contrasto con le prerogative fondamentali dell'individuo[625], come in questo caso.

In sede di verifica del bilanciamento da realizzarsi, in concreto, tra le esigenze di repressione dei reati sottese alla disciplina relativa all'acquisizione dei dati di traffico telefonico e telematico e le garanzie predisposte dagli artt. 7, 8 e 52 della Carta di Nizza, i giudici di Lussemburgo hanno ritenuto che la direttiva 2006/24/CE sulla c.d. *data retention* non superasse il suddetto vaglio di proporzionalità[626]. Siffatto approccio garantista ha, poi, trovato definitivo coronamento nella giurisprudenza successiva della Corte che ha espressamente scolpito un elenco di requisiti minimi a cui gli ordinamenti nazionali sono tenuti ad adeguarsi nel rispetto dei principi enunciati dalla Carta di Nizza[627]. Alla luce di siffatto percorso, i giudici della Corte di Lussemburgo, dunque, non si sono limitati a censurare l'atto di diritto derivato in materia di conservazione dei dati, bensì hanno analizzato le ricadute concrete di siffatta caducazione negli ordinamenti normativi interni[628]. Infine, si è imposto agli Stati membri l'adeguamento delle discipline nazionali di c.d. *data retention* agli *standard* di tutela rilevati in ambito comunitario.

Eppure, gli arresti della Corte di Giustizia non hanno ricevuto la dovuta attenzione dai legislatori nazionali[629] né tantomeno da quello italiano, che ha dimostrato una certa "resistenza"[630] nel recepire le istanze comunitarie in materia di *data retention*. Non diverso è stato l'atteggiamento della giurisprudenza nazionale –

---

[625] In questo senso ANDOLINA, *L'ammissibilità degli strumenti di captazione dei dati personali tra standard di tutela della* privacy *e onde eversive*, in *Arch. pen.*, 2015, n. 3, 936.

[626] Cfr. Corte giust. UE, Gr. Sez., sent. 8 aprile 2014, *Digital Rights Ireland*, *cit.*, punto 71. In dottrina, è stato osservato che la Corte abbia deciso di caducare sin da subito la direttiva, per proteggere in modo più intenso i diritti fondamentali da essa coinvolti. In tal senso, MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale*, *cit.*, 778.

[627] Così LUPÀRIA, Data retention *e processo penale*, *cit.*, 760. Nello stesso senso, MARCOLINI, *L'istituto della* data retention *dopo la sentenza della corte di giustizia del 2014*, *cit.*, 1589.

[628] Sul punto v. FLOR, *La Corte di giustizia considera la direttiva europea 2006/24 sulla cd*. "data retention" *contraria ai diritti fondamentali. Una lunga storia a lieto fine?* in *Dir. Pen. contemp., 2014*, 188.

[629] Cfr. in proposito, European Digital Rights (EDRi), *EU Member States willing to retain illegal data retention*, in *www.edri.org*. L'European Digital Rights è un'associazione internazionale, con sede a Bruxelles, che si occupa di difendere le libertà e i diritti a livello comunitario e internazionale. Si tratta di un collettivo di ONG, esperti, sostenitori e accademici interessati a promuovere i diritti digitali in tutta Europa.

[630] Sul punto, v. LUPÀRIA, Data retention *e processo penale,* cit., 758. L'Autore sottolinea una «forma di negativa resilienza» del legislatore e della magistratura italiana di fronte alle "svolte garantiste" della giurisprudenza comunitaria. Tale atteggiamento si riscontra nell'esitazione ad attuare le Direttive approvate dall'UE e in una tendenziale impostazione di chiusura rispetto agli orientamenti ermeneutici comunitari.

tanto di merito[631], quanto di legittimità[632] – che ha riservato alle novità provenienti dall'Unione Europea un orientamento ermeneutico di chiusura, volto a negare la pienezza dei diritti fondamentali invocata[633].

In tale sede, è, dunque, opportuno verificare se l'inerzia del legislatore e della giurisprudenza italiana trovino giustificazione nella effettiva compatibilità dell'art. 132 del Codice *Privacy* rispetto alla salvaguardia dei diritti invocata dal quadro sovranazionale o se, invece, sia solo il frutto di un approccio "riduttivo"[634] e inottemperante rispetto alle nuove istanze comunitarie. Una volta messa in luce la contrarietà della disciplina attuale in materia di conservazione dei "dati esterni" rispetto al diritto comunitario, verranno analizzate le ricadute concrete sul nostro ordinamento processuale. Infine, si procederà all'analisi del quadro giurisprudenziale e al tanto atteso *revirement* in materia.

2. Il rapporto tra il diritto dell'Unione europea e gli ordinamenti interni (cenni).

Davanti agli arresti della Corte di Giustizia in materia di *data retention,* diventa esigenza improrogabile valutare l'impatto che siffatte pronunce hanno nel quadro normativo interno. In base ai principi che regolano i rapporti tra l'ordinamento Ue e quello nazionale, qualora sorga un conflitto tra gli stessi, esso deve essere risolto in base al primato del diritto comunitario. Alla luce di siffatto principio, elaborato in sede giurisprudenziale[635], le norme nazionali non possono in alcun modo ostacolare l'applicazione del diritto dell'Unione all'interno degli ordinamenti degli Stati membri[636].

---

[631] Cfr. Cap III § 4.
[632]Cfr. Cap III § 4.
[633] Cfr. CAIANIELLO, *Dal terzo pilastro ai nuovi strumenti: diritti fondamentali, "road map" e l'impatto delle nuove direttive*, in *Dir. pen. cont*, 2015, 78.
[634] In questi termini, LUPÀRIA, Data retention *e processo penale, cit.*, 758.
[635] Il primato del diritto comunitario è stato esplicitato per la prima volta dalla Corte di Giustizia nella sentenza del 15 luglio 1964, Costa c. Enel, in *Racc.*, 1129. Nel caso di specie, il ricorrente contestava la compatibilità della disciplina italiana di nazionalizzazione dell'energia elettrica rispetto al TCE. Nella risoluzione della questione la Corte ha sottolineato «l'impossibilità per gli Stati di far prevalere, contro un ordinamento giuridico da essi accettato a condizione di reciprocità, un provvedimento unilaterale ulteriore, il quale pertanto non potrà essere opponibile all'ordine comune. Se l'efficacia del diritto comunitario variasse da uno Stato all'altro, in funzione delle leggi interne posteriori, ciò metterebbe in pericolo l'attuazione degli scopi del Trattato».
[636] Sul punto, v. DANIELE, AMADEO, *Diritto dell'Unione europea: sistema istituzionale, ordinamento, tutela giurisdizionale, competenze*, Milano, 2020, 326.

Inoltre, come noto[637], i diritti e le libertà previsti nelle Carte internazionali sono riconosciuti come valori fondamentali nel sistema normativo interno[638]. In particolare, i diritti proclamati dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, hanno rango "infra-costituzionale"[639] in quanto sono assimilabili a norme interposte[640] rispetto al principio espresso dall'art. 117, comma 1[641]. Di conseguenza, qualora si riscontri l'incompatibilità tra una disposizione legislativa interna e un articolo della Convenzione sopracitata, i giudici ordinari non possono procedere direttamente alla disapplicazione[642] della norma di diritto interno, ma sono tenuti a sottoporre la questione di legittimità dinanzi alla Corte costituzionale[643]. In tale sede, la Consulta sarà chiamata a valutare se la disposizione legislativa nazionale entri in contrasto con l'art. 117 Cost. nella parte in cui impone la conformazione dell'ordinamento interno ai vincoli derivanti dalla CEDU[644].

---

[637] In tal senso, IOVENE, Data retention *tra passato e futuro. Ma quale presente?* in *Cass. Pen*., 2014, 4278.

[638] Siffatto principio è stato ribadito dalla Corte costituzionale, secondo Convenzione europea e il sistema di garanzie in esso previsto è finalizzato «a garantire una soglia minima di tutela comune, in funzione sussidiaria rispetto alle garanzie assicurate dalle Costituzioni nazionali». Sul punto, v. sent. Corte cost. 24 febbraio 2017, n. 43 su *www.giurcost.org.*

[639] L'espressione è di ANDOLINA, *L'ammissibilità degli strumenti di captazione dei dati personali tra standard di tutela della* privacy *e onde eversive*, *cit.*, 919.

[640] Si utilizza l'espressione "norma interposte" o "parametro interposto" quando si fa riferimento a norme che di per sé non hanno rango costituzionale, ma la cui violazione comporta indirettamente la violazione dei principi costituzionali. Dopo la Riforma costituzionale del Titolo V del 2001, l'art 117, comma 1, Cost. implica che ogni trattato internazionale, tra cui anche la CEDU, possa fungere da parametro interposto nel giudizio di legittimità costituzionale delle leggi ordinarie. È sempre la Costituzione italiana che impone alle leggi il rispetto di tali atti che quindi si "interpongono" tra esse e gli atti legislativi ordinari. Così, v. BIN, PITRUZZELLA, *Diritto costituzionale,* Torino, 2020, 356.

[641] L'art. 117, comma 1, Cost. prevede che «La potestà legislativa è esercitata dallo Stato e dalle Regioni nel rispetto della Costituzione, nonché dei vincoli derivanti dall'ordinamento comunitario e dagli obblighi internazionali». Tale disposizione chiarisce che. Le regole dell'ordinamento europeo e internazionale rappresentano un limite costituzionale della potestà legislativa sia dello Stato, sia delle Regioni.

[642] Quando si parla di "disapplicazione" si fa riferimento all'istituto che sancisce il potere del giudice ordinario di non applicare un atto normativo o amministrativo quando questo entri in contrasto con le fonti di rango superiore.

[643] Per un approfondimento sul rapporto problematico tra le fonti comunitarie e internazionali e il diritto italiano v. STROZZI, MASTROIANNI, *Diritto dell'Unione europea. Parte istituzionale*, Torino, 2020, 453 e ss.

[644] Il meccanismo di cui *supra* è stato illustrato chiaramente nella sent. Corte cost. 22 ottobre 2007, n. 349, su *www.cortecostituzionale.it*. In tale sede, la Consulta affermato che «Al giudice comune spetta interpretare la norma interna in modo conforme alla disposizione internazionale, entro i limiti nei quali ciò sia permesso dai testi delle norme. Qualora ciò non sia possibile, ovvero dubiti della compatibilità della norma interna con la disposizione convenzionale "interposta", egli deve investire questa Corte della relativa questione di legittimità costituzionale rispetto al parametro dell'art. 117, primo comma». Per un approfondimento sul contenuto della sentenza sopra citata, *ex multis* v. ZANGHÌ, *La Corte costituzionale risolve un primo contrasto con la Corte europea dei diritti dell'uomo ed interpreta l'art. 117 della Costituzione: le sentenze n. 348 e 349 del 2007*, disponibile *online* su *www.giurcost.org*;

La Carta di Nizza, invece, fa parte del diritto primario dell'Unione europea e, in base all'art. 6 TUE[645] che le attribuisce lo stesso valore giuridico dei Trattati, ha efficacia diretta e vincolante per gli Stati membri[646] nelle materie di competenza dell'Unione (art. 51 CDFUE)[647]. Essa assume nella gerarchia delle fonti interne una posizione para-costituzionale in quanto riconosce ulteriori parametri di legittimità, sostanziali e processuali, delle normative interne[648]. Ciò posto, qualora si riscontri un contrasto tra una disposizione interna e il sistema di tutele previsto dalla Carta di Nizza, così come interpretato dalla Corte di Giustizia[649], il giudice ordinario ha la possibilità di disapplicare la prima, senza passare attraverso il vaglio del Giudice delle leggi[650].

Una volta delineato siffatto scenario, è opportuno valutare se la versione attuale dell'art. 132 del Codice *Privacy* sia conforme agli artt. 7 e 8 e 52 della Carta di Nizza, così come interpretati dalla Corte di Giustizia, e se soddisfi gli *standard* di tutela in punto di proporzionalità[651], determinatezza e stretta necessità. Più nello specifico, è

PUSTORINO, *Corte costituzionale, Cedu e controlimiti (Nota a Corte cost., 28 novembre 2012, n. 264, Inps c. Lorenzon)*, in *Giur. it.*, 2013, 770; CARTABIA, *Le sentenze «gemelle»: diritti fondamentali, fonti, giudici*, in *Giur. cost.*, 2007, 3564.

[645] L'art. 6, par. 1, della Carta di Nizza, così come modificato dal Trattato di Lisbona, stabilisce che: «L'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, adattata il 12 dicembre 2007 a Strasburgo, che ha lo stesso valore giuridico dei trattati.
Le disposizioni della Carta non estendono in alcun modo le competenze dell'Unione definite nei trattati. I diritti, le libertà e i principi della Carta sono interpretati in conformità delle disposizioni generali del titolo VII della Carta che disciplinano la sua interpretazione e applicazione e tenendo in debito conto le spiegazioni cui si fa riferimento nella Carta, che indicano le fonti di tali disposizioni».

[646] In tal senso, IOVENE, Data retention *tra passato e futuro. Ma quale presente?* in *Cass. Pen*., 2014, 4278.

[647] L'art 51, par 2, della Carta di Nizza prevede che: «La presente Carta non estende l'ambito di applicazione del diritto dell'Unione al di là delle competenze dell'Unione, né introduce competenze nuove o compiti nuovi per l'Unione, né modifica le competenze e i compiti definiti nei trattati».

[648] In tal senso, ANDOLINA, *L'ammissibilità degli strumenti di captazione dei dati personali tra standard di tutela della* privacy *e onde eversive*, *cit.*, 919.

[649] L'interpretazione del diritto europeo fornita in sede di rinvio pregiudiziale (art. 267 TFUE) dalla Corte di Giustizia è vincolante per tutti gli Stati membri, che non possono discostarsene. Inoltre, nel caso in esame, la Corte di giustizia non si è limitata a fornire un'interpretazione della direttiva della *data retention*, ma l'ha annullata, privandola di qualsiasi effetto a livello comunitario. Per quanto riguarda il "nuovo" ruolo della «giurisprudenza-fonte» e le conseguenze che esso produce sul diritto penale nel suo complesso, v. DONINI, *Europeismo giudiziario e scienza penale. Dalla dogmatica classica alla giurisprudenza-fonte*, Milano, 2011.

[650] Sul punto v. Corte cost., 11 marzo 2011, n. 80, in *Giur. cost*., 2011, 1224. In tale sede, la Consulta ha confermato il diverso rango della CEDU rispetto alla CDFUE, riconoscendo soltanto a quest'ultima la diretta applicabilità nell'ordinamento nazionale.

[651] Il principio di proporzionalità richiamato dalla clausola dell'art. 52, par. 1, della Carta di Nizza ha assunto un significato peculiare e differente da quello che ha nell'ambito dell'art. 5, par. 4, TUE. Per la configurazione del principio di proporzionalità come principio cardine nel quadro comunitario: v. Corte giust. UE, Gr. Sez., 9 novembre 2010, *Volker und Markus Schecke e Eifert*; Corte giust. UE, Gr. Sez.,

necessario verificare se l'attività di acquisizione dei dati di traffico, così come prevista dalla normativa italiana vigente, realizzi un sacrificio della "sfera privata" dell'individuo in linea con le garanzie individuate dai giudici di Lussemburgo.

In caso contrario, qualora risulti evidente l'incompatibilità della disciplina italiana in materia di *data retention* rispetto al sistema di tutele di provenienza comunitaria, potrà essere oggetto di disapplicazione da parte del giudice ordinario. A tale fine, seguirà un'analisi dei profili di criticità dell'art. 132 del Codice *Privacy*.

3. L'impatto delle pronunce della Corte di Giustizia Ue sul quadro normativo nazionale.

In primo luogo, la contravvenzione da parte della norma sopracitata all'elementare esigenza di proporzione tra l'interesse alla persecuzione dei reati e la libertà dell'individuo è desumibile del fatto che il legislatore nazionale ha optato per la previsione di un obbligo "generale" di conservazione dei dati[652], senza restringere la portata della norma ai reati "gravi"[653]. L'esigenza di limitare la possibilità di accedere ai dati relativi al traffico da parte delle pubbliche autorità soltanto nella lotta contro gravi forme di criminalità, è stata ribadita nella recentissima sentenza *H.K. Danmark*[654]. Come si è anticipato, in tale sede, la Corte di Giustizia ha affermato che l'ingerenza grave nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta di Nizza può essere giustificata soltanto laddove si persegua l'obiettivo di accertare e reprimere fattispecie delittuose altrettanto "gravi"[655]. Laddove sia stabilito diversamente, come nella normativa italiana, non può considerarsi rispettato il principio di proporzionalità[656].

---

29 gennaio 2008, causa C-275/06, *Promusicae e Telefonica de Espana Sau*. Sul punto, v. anche TESAURO, *La ragionevolezza nella giurisprudenza comunitaria*, Napoli, 2012, 43.

[652] Cfr. art. 132 comma 1. Per un approfondimento sul punto si rinvia al Cap. I.

[653]Cfr. FLOR, *La Corte di giustizia considera la direttiva europea 2006/24 sulla cd*. "data retention" *contraria ai diritti fondamentali, cit.,* 189. Corte giust. UE, sent. 2 ottobre 2018, *Ministerio Fiscal*, *cit*., punto 54.

[654] Per approfondimento sul contenuto della pronuncia si rinvia al Cap. II.

[655] Cfr. Corte giust. UE, Gr. Sez., sent. 2 marzo 2021, *H.K. Danmark, cit.*, punto 33. In tale sede, la Corte di Giustizia afferma 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 sanciti dagli articoli 7 e 8 della Carta, come quelle che comporta la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione, sia questa generalizzata e indifferenziata oppure mirata».

[656] Sul punto si veda, Corte giust. UE, Gr. Sez., sent. 2 marzo 2021, *H.K. Danmark, cit.*, punto 35. In conformità, si veda anche Corte giust. UE, sent. del 6 ottobre 2020, *La Quadrature du Net* e a., cit., punti 140 e 146; Corte giust. UE, sent. 2 ottobre 2018, *Ministerio Fiscal*, *cit*., punto 54.

In secondo luogo, l'art. 132, commi 1 e 1-*bis*, prevede l'archiviazione dei dati di traffico telefonico e telematico di chiunque si avvalga dei servizi di comunicazione elettronica, senza alcuna deroga o limitazione. Questo trova applicazione in maniera «generalizzata» e «indifferenziata», anche nei confronti di coloro tra i quali non esiste alcun collegamento, neppure indiretto, rispetto a violazioni penali o minacce per la sicurezza pubblica. Inoltre, l'attività di conservazione prevista nel Codice *Privacy* non è limitata ad una «zona geografica» o «ristretta cerchia di persone»[657] implicate in un procedimento penale o che comunque potrebbero contribuire nella lotta contro la criminalità, obiettivo ultimo della c.d. *data retention*.

Come affermato nella sentenza *Tele2 Sverige*[658], una normativa nazionale che non delimiti la portata della misura di conservazione dei dati a titolo preventivo, non può considerarsi giustificata alla luce del principio dello «stretto necessario», così come richiede l'art. 15, paragrafo 1, della direttiva 2002/58/CE, interpretato alla luce degli articoli 7, 8 e 52 della Carta di Nizza[659].

In terzo luogo, la normativa italiana non impone ai fornitori dei servizi di comunicazione il rispetto di particolari misure di sicurezza, volte a tutelarne l'integrità e ad evitare rischi di abuso o accesso non autorizzato.[660]L'adozione di specifici accorgimenti idonei a garantire un "elevato" livello di protezione dei dati di traffico è

---

[657] Sul punto Corte giust. UE, Gr. Sez., sent. 21 dicembre 2016, *Tele2 Sverige*, *cit.*, punti 105 e 109. Secondo i giudici di Lussemburgo «siffatta delimitazione può essere ottenuta mediante un criterio geografico qualora le autorità nazionali competenti considerino, sulla base di elementi oggettivi, che esiste, in una o più zone geografiche, un rischio elevato di preparazione o di commissione di atti di questo tipo».Vedi per analogia Corte giust. UE, Gr. Sez., sent. 8 aprile 2014, *Digital Rights*, *cit.*, punto 54.

[658] Per l'analisi puntuale del contenuto della sentenza sopracitata si rinvia ala Cap. II § 10.

[659] Cfr. Corte giust. UE, Gr. Sez., sent. 21 dicembre 2016, *Tele2 Sverige*, *cit.*, punto 112.

[660] Con i provvedimenti del 17 gennaio 2008, 24 luglio 2008 e 29 aprile 2009, il Garante della *Privacy* ha prescritto in capo ai *providers* una serie di adempimenti aventi ad oggetto, ad esempio, prescrizioni per l'adozione di sistemi di autenticazione e autorizzazione, di cifratura e protezione, nonché per la conservazione separata dei dati. Tali prescrizioni, però, pur apparendo stringenti, e pur risultando rilevanti nella materia oggetto di studio, lasciano di fatto al fornitore la determinazione concreta delle procedure tecniche da adottare. Le stesse misure di *audit* originariamente prescritte risultano generiche e fanno riferimento alla «garanzia di completezza, non modificabilità e autenticità delle registrazioni», o all'adozione di «dispositivi non alterabili», oppure ad espressioni del tipo «prima della scrittura, i dati o i raggruppamenti di dati devono essere sottoposti a procedure informatiche per attestare la loro integrità, basate sull'utilizzo di tecnologie crittografiche». Tali prescrizioni esprimono le difficoltà del legislatore nonché del Garante ad imporre oltre all'obbligo di conservazione dei dati, ulteriori adempimenti che comportino impegni organizzativi, strutturali ed economici per i gestori di servizi di comunicazione elettronica. È possibile consultare i documenti del Garante della *Privacy* sopracitati in *www.garanteprivacy.it*.

rimessa alla discrezionalità dei *service providers,* che non sono nemmeno tenuti a conformarsi alle *best practice*s riconosciute a livello internazionale.

Inoltre, l'art 132, comma 3[661], del Codice *Privacy* riconosce al pubblico ministero il potere acquisire i dati di traffico, senza subordinare il suddetto accesso al controllo preventivo di un organismo terzo e indipendente[662] (il giudice). La norma, dunque, attribuisce al medesimo organo a cui spetta la conduzione dell'indagine penale e la raccolta di elementi di prova a carico dell'imputato la decisione di acquisire ulteriori elementi potenzialmente idonei a sostenere l'accusa. Come si dirà in seguito, siffatta incongruenza è stata più volte sottoposta al vaglio della Corte di cassazione, la quale ha, però, sempre negato l'incompatibilità rispetto al diritto comunitario[663].

Alla luce della recentissima sentenza *H.K. Danmark*, risulta molto arduo – se non impossibile – sostenere siffatta tesi della giurisprudenza.

In tale sede, la Corte di Giustizia ha, infatti, espressamente sottolineato la necessità che l'accesso delle autorità nazionali competenti ai dati "esterni" alla comunicazione sia subordinato al vaglio preventivo di un giudice o di un'autorità indipendente, che disponga di tutte le garanzie necessarie per conciliare i diversi interessi in gioco. In particolare, tale attività di controllo deve essere affidata ad un organo «obiettivo» e «imparziale»[664], che non risenta di alcuna «influenza esterna» e non sia coinvolta nella conduzione dell'indagine penale in corso. Tali condizioni non risultano soddisfatte nel caso del P.M. il quale, privo dello «status di terzo rispetto agli interessi in gioco»[665], ha il compito di esercitare l'azione penale unicamente in base alla legge e al suo convincimento.

In base alle suddette osservazioni, l'art. 132, comma 3, del Codice *Privacy* che attribuisce al pubblico ministero il compito di autorizzare l'accesso ai dati

[661] Per un approfondimento sulla procedura di acquisizione dei dati di traffico predisposta nel Codice *Privacy* si rinvia al Cap I § 4.3.
[662] Sulla terzietà e imparzialità si veda quanto affermato *infra*.
[663] In particolare, si fa riferimento alla sentenza analizzata nel Cap. III § 4.2.
[664] Cfr. Corte giust. UE, Gr. Sez., sent. 2 marzo 2021, *H.K. Danmark, cit.*, punti 52 e 53. In conformità si veda anche Corte giust. UE, Gr. Sez., sent. 21 dicembre 2016, *Tele2 Sverige*, *cit.*, punto 125; Corte giust. UE, Gr. Sez., sent. 8 aprile 2014, *Digital Rights*, *cit.*, punto 62.
[665] Cfr. Corte giust. UE, Gr. Sez., sent. 2 marzo 2021, *H.K. Danmark, cit.*, punti 56 e 57.

relativi al traffico non può dirsi compatibile rispetto agli articoli 7, 8 nonché 52 della Carta di Nizza[666].

Il quinto elemento che depone a favore dell'inconciliabilità tra la disciplina italiana in tema di *data retention* e gli arresti della giurisprudenza europea riguarda l'assenza di previsione di requisiti sostanziali e procedurali che legittimino l'acquisizione dei dati di traffico[667]. Ai sensi dell'art 132, comma 3, del Codice *Privacy,* è, infatti, consentito l'acceso a tutti i dati conservati indipendentemente dal fatto che l'istanza dell'organo inquirente si fondi su criteri oggettivi che giustifichino la decisione di disporre la misura preventiva. L'attività acquisitiva non risulta, dunque, subordinata né al *fumus commissi delicti*[668] né alla sussistenza di un nesso tra l'utenza di cui si richiedono i tabulati e il reato presupposto. Pertanto, l'istituto che prevede un accesso generale a tutti i dati conservati a prescindere dall'esistenza di un legame con la finalità perseguita dell'accertamento e della repressione dei reati, non può considerarsi limitato allo «stretto necessario», né tantomeno conforme al principio di proporzionalità[669].

Da ultimo, risulta assai problematica la previsione del legislatore italiano circa i tempi di conservazione dei dati. Come si è già avuto modo di approfondire[670], l'art. 132, comma 1 e 1-*bis* del Codice *Privacy*, impone ai fornitori dei servizi di comunicazione elettronica di archiviare i dati di traffico telefonico per 24 mesi; i dati di traffico telematico per 12 mesi; i dati relativi alle chiamate senza risposta per

---

[666] Inoltre, siffatta previsione risulta incompatibile non soltanto con il diritto comunitario ma anche lo statuto costituzionale previsto dagli artt. 14 e 15 Cost. Come si è già visto nel Cap. II, a cui si rinvia, il legislatore italiano può adottare misure in deroga all'inviolabilità del domicilio e alla segretezza delle comunicazioni soltanto qualora sia rispettato il doppio requisito della riserva di legge e della riserva di giurisdizione. Di conseguenza, il potere del pubblico ministero di disporre l'acquisizione dei dati di traffico, in via autonoma e senza il previo controllo dell'autorità giurisdizionale, risulta in contrasto con le garanzie costituzionali.

[667] Sul punto, vedi Corte giust. UE, Gr. Sez., sent. 21 dicembre 2016, *Tele2 Sverige*, *cit.*, punto 118. Secondo i giudici di Lussemburgo, la normativa nazionale in tema di *data retention* deve prevedere «condizioni sostanziali e procedurali che disciplinano l'accesso delle autorità nazionali competenti ai dati conservati». In conformità v. Corte giust. UE, Gr. Sez., sent. 8 aprile 2014, *Digital Rights*, *cit.*, punto 61.

[668] Si fa qui riferimento al *fumus commissi delicti* integrato dalla acquisizione di una notizia di reato. In riferimento a tale concetto si parla, rispettivamente, di «presupposto sostanziale», ovvero di «un fatto processuale a ricadute sostanziali». Sul punto, v. CAIANELLO, *Il principio di proporzionalità nel processo penale, cit.*, 143.

[669] Cfr. Corte giust. UE, Gr. Sez., sent. 21 dicembre 2016, *Tele2 Sverige*, *cit.*, punto 116.

[670] Sul punto, si rinvia al Cap. I.

soli 30 giorni. Sorvolando sulla decisione[671] di differenziare i periodi di conservazione in base alla tipologia di dati e non alla gravità dei reati presupposto per cui si procede, le tempistiche prescelte risultano, tutto sommato, compatibili rispetto al quadro comunitario in materia di *data retention*[672].

Lo scenario si complica, però, con la novella del 2018[673] mediante la quale il legislatore italiano ha esteso a sei anni il periodo di conservazione di tutti i dati telefonici e telematici. Sebbene tale dilatazione dei tempi di archiviazione risulti, infatti, apparentemente limitato all'accertamento di reati consumati o tentati ricompresi negli articoli 51 comma 3-*quater* c.p.p. e 407 comma 2 lett. a) c.p.p, questo deve ritenersi esteso, di fatto, nei confronti di qualsiasi reato per cui si procede. Come si è affermato in precedenza, dunque, l'inserimento del comma 5-*bis* nell'art. 132 del Codice *Privacy* ha, in sostanza, eroso la portata applicativa dei commi 1 e 1-*bis* sopracitati.

Siffatta constatazione[674], deriva dal fatto che i fornitori dei servizi di comunicazione, quando adempiono all'obbligo di conservazione dei dati, non sanno né se i tabulati saranno acquisiti dall'autorità giudiziaria né per quali tipologie di reati sarà richiesto l'accesso. Di conseguenza, i *service providers* sono tenuti indirettamente a conservare tutti i dati per un periodo complessivo di sei anni, nell'eventualità che gli organi inquirenti ne facciano richiesta ai sensi dell'art. 132,

---

[671] In dottrina, sono state espresse perplessità sulla scelta del legislatore di differenziare i periodi di conservazione dei dati in base alla provenienza degli stessi da SIGNORATO, *Novità in tema di* data retention*. La riformulazione dell'art. 132 codice privacy da parte del D. Lgs. 10 agosto 2018 n. 101*, in *Dir. Pen. contemp.*, 2018, 16. Inoltre, l'Autrice critica il fatto che le tempistiche non siano in nessuno modo calibrate rispetto alla gravità dei delitti o la tipologia dei reati per cui si procede.

[672] Sul punto, si faccia riferimento alla Relazione della Commissione europea del 18 aprile 2011. Per visionare il testo in versione integrale si veda COM (2011) 225 definitivo su *www.eur-lex.europa.eu.* In particolare, si rinvia alla Tabella 3 che riporta i "Periodi di conservazione previsti dalla legislazione nazionale" di tutti gli Stati membri.

[673] Si fa riferimento all'art. 132, comma 5-*bis*, del Codice *Privacy* inserito con il d.lgs. 10 agosto 2018, n. 101. Il comma sopracitato rinvia espressamente all'articolo 24 della legge europea 167/2017 ai sensi della norma sopracitata: «In attuazione dell'articolo 20 della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio, al fine di garantire strumenti di indagine efficace in considerazione delle straordinarie esigenze di contrasto del terrorismo, anche internazionale, per le finalità dell'accertamento e della repressione dei reati di cui agli articoli 51, comma 3-quater, e 407, comma 2, lettera a), del codice di procedura penale il termine di conservazione dei dati di traffico telefonico e telematico nonché dei dati relativi alle chiamate senza risposta, di cui all'articolo 4-bis, commi 1 e 2, del decreto-legge 18 febbraio 2015, n. 7, convertito, con modificazioni, dalla legge 17 aprile 2015, n. 43, è stabilito in settantadue mesi, in deroga a quanto previsto dall'articolo 132, commi 1 e 1-bis, del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196».

[674] In dottrina, v. RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico, cit.,* 162.

comma 5-*bis*[675]. Il regime emergenziale introdotto con la legge europea del 2017 e finalizzato ad agevolare la repressione dei reati gravi e di matrice terroristica diventa, di fatto, regime ordinario e oggetto di applicazione indifferenziata[676].

Le criticità di tale disciplina, evidenti *ictu oculi*, erano state rilevate già prima dell'approvazione della legge europea del 2017[677] dall'allora Presidente del Garante della *Privacy,* Antonio Soro. A margine della sua audizione dinanzi al COPASIR[678], il Presidente ne ha sottolineato il «palese contrasto con l'ordinamento e con la giurisprudenza dell'unione europea»[679]. A tal proposito, ha spiegato che, sebbene il terrorismo rappresenti un obiettivo di interesse generale e, dunque, volto a legittimare di per sé la conservazione dei dati di traffico, la giurisprudenza europea vieta espressamente una raccolta generale e indiscriminata. Gli obblighi di raccolta dei dati esterni per finalità di accertamento di reati gravi devono, dunque, essere «limitati temporalmente in misura proporzionata alle esigenze investigative»[680]. Tale assunto non viene rispettato nel caso in cui l'attività di archiviazione dei dati sia estesa in modo generalizzato a sei anni. Sulla base di tali osservazioni, il Presidente ha ribadito l'esigenza di ricondurre la normativa in fase di approvazione al principio di proporzionalità.

Intervenuto nuovamente sull'argomento il 24 ottobre 2017[681], il Presidente Soro ha aggiunto che la decisione di aumentare fino a sei anni il periodo di *data storage* risulta «incomprensibile» non solo alla luce degli arresti della Corte di

---

[675] L'argomento è stato oggetto di approfondimento nel Cap. I, a cui si rinvia.

[676] Sul punto, v. BERRUTI, *Un* vulnus *al diritto alla* privacy *per la lotta contro il terrorismo*, 15 gennaio 2016, su *www.legislazionepenale.eu*; CAPUTO, *La conservazione dei dati di traffico telefonico e telematico nella normativa antiterrorismo*, in *Arch. pen.*, 2016, 1; FILIPPI, *Intercettazioni, tabulati e altre limitazioni della segretezza delle comunicazioni*, in *Procedura penale. Teoria e pratica del processo*, SPANGHER, MARANDOLA, GARUTI e KALB (diretto da), Torino, 2015, 1132.

[677] Si fa riferimento alla legge che recepisce la Direttiva 2017/54/UE approvata il 15 marzo 2017 recante «modifica della direttiva 2003/87/CE al fine di mantenere gli attuali limiti dell'ambito di applicazione relativo alle attività di trasporto aereo e introdurre alcune disposizioni in vista dell'attuazione di una misura mondiale basata sul mercato a partire dal 2021».

[678] Il Comitato parlamentare per la sicurezza della Repubblica (COPASIR) è un organo bicamerale composto da 5 senatori e deputati, scelti in modo tale da garantire eguale rappresentanza a maggioranza e opposizione. Tale organo è preposto alla verifica in modo sistematico e continuativo del Sistema di informazione per la sicurezza.

[679] Si fa riferimento al Comunicato stampa rilasciato in data 25 luglio 2017 (Doc. 6651715), disponibile *online* su *wwww.garanteprivacy.it.*

[680] Si veda la nota precedente.

[681] L'intervento del Presidente Soro si è tenuto durante il convegno "Privacy digitale e protezione dei dati personali tra persona e mercato", svoltosi a Firenze il 24 ottobre 2017. È possibile prendere visione del video-intervento integrale a cui si fa riferimento su *www.key4biz.it.*

Giustizia, ma soprattutto perché da siffatta estensione temporale possono derivare gravi lesioni alla *privacy* dei cittadini italiani[682]. Sul punto, ha, infatti, evidenziato che più a lungo sono archiviati i dati nei *server* dei fornitori dei servizi di comunicazione, maggiore è il rischio che questi siano oggetto di *data breach* [683] e di indebito utilizzo. Inoltre, il Presidente ha evidenziato che la decisione di conservare per 6 anni tutti i dati di traffico telefonico e telematico, che ammontano all'incirca a 5 miliardi al giorno[684], stravolge la medesima natura della *data retention,* che da mezzo di ricerca della prova diventa «misura massiva»[685]. Per le ragioni sopra esposte, ha, dunque, auspicato la revisione di una disciplina che, nella formulazione attuale, contravviene al principio di proporzionalità tra esigenze investigative e protezione dei dati[686].

4. L'atteggiamento di "resistenza" della giurisprudenza nazionale.

Alla luce delle osservazioni di cui *supra,* emerge con chiarezza che la disposizione italiana *de jure condito* in materia di conservazione dei dati di traffico compromette, ben oltre il limite del «contenuto essenziale»[687] e del principio di proporzionalità, il rispetto dei diritti fondamentali previsti dalla Carta di Nizza[688].

---

[682] Sul punto, il Presidente del Garante della *Privacy* ha affermato che «Se la minaccia di attacchi informatici è quotidiana, diventa ancora più incomprensibile la scelta presa recentemente dal Parlamento (dalla Camera n.d.r.): la decisione di aumentare fino a 6 anni la *Data Retention*, ignorando, non solo le sentenze della Corte di giustizia europea, ma anche il buon senso di rendere governabili le banche dati pubbliche e private degli operatori telefonici e telematici».

[683] Per la definizione di «data breach» o «violazione dei dati personali», si faccia riferimento all'art. 4, punto 12, del GDPR secondo cui «la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati». Sul punto, si faccia riferimento anche al Considerando 85.

[684]Sul punto, Antonio Soro ha ribadito che «Al giorno sono circa 5 miliardi i dati di traffico telefonico e telematico conservati dagli operatori e dagli Internet Service Provider e questa prassi di conservarli per 6 anni in modo indistinto andrebbe nella direzione opposta di proteggere la privacy del nostro Paese e dei cittadini».

[685] Il rischio che tramite l'istituto della *Data Retention* si realizzi un meccanismo di «mass surveillance» era già stato evidenziato nella sentenza del 2 marzo 2010 del *Bundesverfassungsgericht, sez III (1BvR 256/08).* Per un approfondimento sul punto si rinvia al Cap. II § 8.1.

[686] In termini analoghi si è espresso il Presidente del Garante della *Privacy* europeo, Giovanni Buttarelli, durante la presentazione della relazione annuale dell'*European Data Protection Supervisor* illustrata il 28 febbraio 2019 davanti la Commissione per le libertà civili, la giustizia e gli affari interni del Parlamento europeo. In tale sede, il Presidente Buttarelli ha affermato che la legge sulla Data Retention in vigore in Italia fino a 6 anni sia «un grave errore» e «incompatibile con i valori europei».

[687] Cfr. Corte giust. UE, Gr. Sez., sent. 8 aprile 2014, *Digital Right. Ireland*, *cit.*, punto 38.

[688] In dottrina, siffatta tesi è espressa chiaramente, *ex multis*, da FLOR, *La Corte di giustizia considera la direttiva europea 2006/24 sulla cd*. "data retention" *contraria ai diritti fondamentali, cit.,* 189; PASCALI, *La* data retention *dopo la dichiarazione di invalidità della Direttiva 2006/24/CE*, *cit.*, 87;

Ne consegue che, l'art. 132 del Codice *Privacy*, già più volte modificato[689], non è attualmente idoneo ad assicurare il rispetto degli *standard* elaborati dalla Corte di Giustizia. Davanti a siffatto scenario, sarebbe auspicabile l'intervento del legislatore italiano, il quale dovrebbe adoperarsi nella modifica della normativa attuale in tema di *data retention* per adeguarla alle istanze di provenienza comunitaria[690]. Soprattutto alla luce delle recentissime pronunce dei giudici di Lussemburgo[691], l'inerzia dello stesso risulta ingiustificata e rivela un atteggiamento di generale "indifferenza" rispetto alle indispensabili esigenze in tema di diritti fondamentali.

In mancanza di un intervento del legislatore, siffatto contrasto può essere risolto soltanto mediante la disapplicazione[692] della disciplina nazionale in materia di *data retention* da parte dei giudici ordinari[693]. A questo punto, assume, dunque, un ruolo fondamentale la giurisprudenza nazionale, ultima possibilità perché si garantisca l'operatività diretta di quanto sancito a livello sovranazionale.

Eppure, anche da parte della giurisprudenza italiana si è riscontrato un diffuso atteggiamento di "resistenza"[694] dinanzi ai principi di diritto enunciati dalla Corte di Giustizia, secondo cui si è sempre negato il contrasto tra questi ultimi e l'art. 132 del Codice *Privacy*. Soltanto di recente[695], si è assistito al tanto atteso *revirement* dei giudici nazionali che ha portato all'emanazione di una domanda di rinvio pregiudiziale ai sensi dell'art. 267 TFUE dinanzi ai giudici di Lussemburgo.

RUGGIERI, Data retention *e giudice di merito penale. Una discutibile pronuncia*, in *Cass. pen*., 2017, 2483.

[689] Per l'evoluzione legislativa avente ad oggetto l'art. 132 del Codice *Privacy* si rimanda al Cap. I.

[690] L'imminente intervento del legislatore ordinario è richiesto da FLOR, *La Corte di giustizia considera la direttiva europea 2006/24 sulla cd*. "data retention" *contraria ai diritti fondamentali, cit.,* 189. L'Autore sottolinea l'esigenza di un intervento del legislatore europeo, nell'ambito di una più ampia politica criminale dell'Unione.

[691] In particolar modo, si fa riferimento alla Corte giust. UE, Gr. Sez., sent. 2 marzo 2021, *H.K. Danmark, cit*.

[692] Per la nozione di "disapplicazione" si veda quanto affermato *supra*.

[693] Infatti, sulla base di quanto accennato in precedenza, qualora insorga un contrasto tra una normativa nazionale e i principi espressi dalla Carta di Nizza e questo non possa essere risolto tramite "interpretazione conforme", la normativa nazionale può essere oggetto disapplicazione diretta da parte del giudice ordinario. Nel senso che l'art. 132 del Codice *Privacy* debba essere oggetto di disapplicazione da parte dei giudici italiani, v. MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale*, *cit.*, 778; in senso analogo, IOVENE, Data retention *tra passato e futuro. Ma quale presente?* in *Cass. Pen*., 2014, 4276; LUPÀRIA, Data retention *e processo penale*, *cit.*, 754.

[694] In merito all'atteggiamento di "resistenza" del legislatore e della giurisprudenza nazionale si veda quanto affermato *supra*.

[695] Il punto verrà approfondito *infra*.

Di seguito, si ripercorreranno le tappe essenziali dell'*iter* affrontato dalla giurisprudenza nostrana per arrivare a siffatta significativa svolta esegetica[696].

4.1 Il Tribunale di Padova: un approccio "conservatore".

In primo luogo, è da segnalare una delle prime pronunce dei giudici di merito in materia di acquisizione dei dati di traffico all'interno di un procedimento penale in corso. Nel caso di specie[697], l'avvocato della difesa, mediante il deposito di una memoria di parte[698], ha eccepito dinanzi al Tribunale di Padova l'inutilizzabilità probatoria[699] di tutti i dati di traffico telefonico acquisiti durante le indagini dal pubblico ministero ai sensi dell'art. 132, comma 3[700], del Codice *Privacy*. In subordine, la difesa ha chiesto la sospensione del procedimento in corso, ai sensi dell'art. 267 TFUE[701] e la sottoposizione alla Corte di Lussemburgo della seguente questione pregiudiziale: «se gli artt. 7, 8 e 52, par. 1 della Carta dei diritti fondamentali dell'Unione europea ostino ad una normativa nazionale, quale l'art. 132 Cod. *Privacy*, che consente l'acquisizione e la conservazione dei dati esterni del traffico telefonico e telematico per qualsiasi tipo di reato».

L'ordinanza[702] di risposta del Tribunale merita di essere segnalata in quanto rivela appieno l'atteggiamento di "resistenza" [703] della magistratura italiana di cui

---

[696] L'espressione è di DELLA TORRE, *L'acquisizione dei tabulati telefonici nel processo penale dopo la sentenza della Grande Camera della Corte di Giustizia UE: la svolta garantista in un primo provvedimento del G.i.p. di Roma*, 2021, su *www.sistemapenale.it.*

[697] Si fa riferimento al Trib. Padova, ord. 15 marzo 2017, Pres. Marassi, in *Dir. pen. cont*., 29 marzo 2017, con nota critica di FLOR, Data retention *ed art. 132 Cod*. privacy: vexata quaestio (?), 356. V. anche F. RUGGIERI, Data retention *e giudice di merito penale. Una discutibile pronuncia*, in *Cass. pen*., 2017, 6, 2483 ss.

[698] Si fa riferimento alla memoria presentata ai sensi dell'art. 121 c.p.p. secondo cui: «In ogni stato e grado del procedimento le parti e i difensori possono presentare al giudice memorie o richieste scritte, mediante deposito nella cancelleria. Sulle richieste ritualmente formulate il giudice provvede senza ritardo e comunque, salve specifiche disposizioni di legge, entro quindici giorni».

[699] Si tratta dell'inutilizzabilità probatoria prevista dall'art. 191 c.p.p. che sanziona l'acquisizione di. prove in violazione dei divieti previsti dalla legge e che può essere rilevata in ogni stato e grado del procedimento penale. Nel caso di specie, il divieto probatorio *ex* art. 191 c.p.p. sarebbe rinvenibile nella violazione di un diritto definito inviolabile dalla Carta di Nizza, norma interposta a Costituzione. Sull'inutilizzabilità probatoria rispetto ai profili di contrarietà al diritto comunitario e costituzionale si tornerà in seguito.

[700] Per il testo dell'articolo sopracitato si rinvia al Cap. I.

[701] Il testo integrale della norma sopracitata è stato riportato *supra.* Per un approfondimento sul funzionamento del rinvio pregiudiziale e sulle sue finalità si rimanda al Cap. II, *nota 210*.

[702] È possibile consultare il testo integrale dell'ordinanza in *Dir. pen. cont*., 29 marzo 2017.

[703] Sul punto, LUPÀRIA, Data retention *e processo penale*, *cit.*, 758.

si è fatto cenno poco sopra[704]. Nella pronuncia *de qua*, i giudici di primo grado hanno affermato che la disciplina della *data retention* contenuta nel Codice *Privacy* perfettamente sia compatibile con il diritto Ue, così come interpretato nelle sentenze *Digital Rights Ireland* e *Tele 2 Sverige*, senza considerare opportuno rimettere la questione ai giudici della Corte di Giustizia[705] .

Per giungere a tale conclusione, i giudici hanno seguito un *iter* argomentativo che è utile ripercorrere sinteticamente.

In primis, hanno riportato il *dictum* della Corte di Lussemburgo nella sentenza *Digital Rights Ireland*, richiamata dalla difesa. Di seguito, hanno, però, sottolineato che la sentenza in questione non abbia alcuna rilevanza nel procedimento penale in oggetto. Infatti, secondo il Collegio, il Codice *Privacy,* entrato in vigore antecedentemente, non potrebbe essere considerato atto di recepimento della direttiva[706] annullata dalla Corte di Giustizia. L'invalidità della stessa non si potrebbe, dunque, trasmettere alla normativa italiana sulla conservazione dei dati di traffico delle comunicazioni.

---

[704] Peraltro, la pronuncia dei giudici di primo grado giunge in un momento storico in cui il rapporto tra l'ordinamento nazionale e il diritto europeo è oggetto di intensa discussione nello "storico" caso Taricco. Si fa qui riferimento Corte di giustizia UE, Gr. Sez., sent. 8 settembre 2015, Taricco (C-105/14). Per un approfondimento sul punto, si vedano, *inter alios*, PULITANÒ, *La posta in gioco nella decisione della Corte costituzionale sulla sentenza Taricco*, in *Dir. pen. cont*., 2016, 1, 236; VIGANÒ, *Il caso Taricco davanti alla Corte costituzionale: qualche riflessione sul merito delle questioni, e sulla reale posta in gioco*, in consultabile online su *www.penalecontemporaneo.it.*

[705] La Corte di Giustizia ha sostenuto che nessuna regola procedurale interna può privare il giudice nazionale dell'ampia facoltà contemplata dal Trattato di effettuare un rinvio pregiudiziale ai sensi dell'art. 267 TFUE. Sul punto, v. sent. Corte Giust., 5 aprile 2016, Puligienica Facility Esco (PFE) su *www.curia.europa.eu.* Inoltre, la Corte ha ritenuto che l'organo giurisdizionale interno che non decide in ultima istanza debba essere libero, qualora ritenga che la valutazione in diritto formulato dal giudice di rango superiore possa portarlo ad emettere una pronuncia contraria al diritto comunitario, di sottoporre alla Corte di Giustizia le questioni con cui deve confrontarsi. Sul punto, v. sent. Corte Giust., 16 gennaio 1974, *Rheinmühlen Düsseldorf*, in Raccolta, 33; sent. Corte Giust, 9 marzo 2010, ERG, *ivi;* nonché, più di recente, sent. Corte Giust., 11 settembre 2014, A c. B, *ivi,* secondo cui la sentenza interpretativa della Corte è vincolante per il giudice di rinvio anche se essa diverga dalle valutazioni del giudice nazionale di rango superiore.

[706] Ai sensi dell'art 288, par. 3, del TFUE a cui si rinvia, le direttive Ue sono idonee a vincolare gli Stati membri a cui sono dirette – nella maggior parte dei casi, si tratta di tutti i paesi membri– per quanto riguarda il risultato da raggiungere, lasciandoli tuttavia liberi in quanto alla scelta dei mezzi necessari. A differenza dei regolamenti, si tratta, dunque, di atti di diritto derivato non direttamente applicabili ma che richiedono l'emanazione di un atto di recepimento da parte del legislatore nazionale. Per un approfondimento sulla natura delle direttive UE si rimanda a STROZZI, MASTROIANNI, *Diritto dell'Unione europea. Parte istituzionale*, *cit.*, 293 e ss.

In secundis, i giudici italiani hanno affermato che, in ogni caso, il principio di proporzionalità[707] sancito dall'art. 52 della Carta di Nizza e ribadito nella sentenza *Digital Rights Ireland*, sia stato pienamente rispettato nel caso di specie. Infatti, i tabulati telefonici riferiti all'imputato sarebbero stati acquisiti dal P.M. ai fini dell'accertamento di un tentativo di incendio con dolo aggravato[708]. Il pubblico interesse a reprimere tale reato, posto a tutela della sicurezza collettiva, andrebbe, dunque, a giustificare la «restrizione dei diritto alla riservatezza» rappresentata dall'acquisizione dei tabulati[709]. Sulla base delle predette osservazioni, il tribunale ha rigettato l'eccezione di inutilizzabilità e di proposizione della questione pregiudiziale alla Corte di giustizia UE ex art. 267 TFUE.

Il percorso motivazionale dei giudici presenta una serie di criticità che sono state efficacemente evidenziate in dottrina[710].

Innanzitutto, è opportuno sottolineare che, se è vero che la versione originaria dell'art. 132 del Codice della *Privacy* sia entrata in vigore prima della direttiva 2006/24/CE[711], non è altrettanto vero che l'impianto normativo in oggetto non abbia dato, successivamente, attuazione alla direttiva europea. Al contrario, con il d.lgs. 109/2008[712] il legislatore italiano ha introdotto apposite modifiche all'articolo sopracitato, proprio con l'intento di recepire l'atto di provenienza

---

[707] Nell'ordinamento italiano, il canone di proporzionalità, espressamente richiamato dal codice di procedura penale in materia di misure cautelari personali (art. 275 c.p.p.), costituisce un principio cardine dell'intero sistema processuale penale, destinato ad assumere rilevanza a fronte di attività investigative che comprimono i diritti fondamentali della persona, *sub specie* i mezzi di ricerca della prova. Ciò si applica, dunque, anche per la conservazione e acquisizione dei dati di traffico. In dottrina, sul v. ORLANDI, *Garanzie individuali ed esigenze repressive (ragionando intorno al diritto di difesa nei procedimenti di criminalità organizzata)*, in AA.VV. *Studi in ricordo di G. Pisapia. Procedura penale II*, Milano, 2000, 560; CAIANELLO, *Il principio di proporzionalità nel processo penale, cit.*, 143.

[708] Si fa riferimento al combinato disposto degli artt. 423, 425 e 56 del c.p. Il reato di incendio ai sensi dell'art. 423, secondo cui «chiunque cagiona un incendio è punito con la reclusione da tre a sette anni» è inserito nel Titolo VI, dedicato ai delitti contro l'incolumità pubblica.

[709] Sul punto, i giudici del Tribunale di Padova hanno affermato che «Il principio di proporzionalità sancito dall'art. 52 della Carta dei Diritti dell'Ue e ribadito dalla Corte nella menzionata sentenza, è pienamente rispettato nel caso di specie: infatti, i dati del traffico telefonico sono stati acquisiti dall'Accusa ai fini dell'accertamento del reato di tentato incendio doloso aggravato (artt. 56, 61 n.5, 110, 423, 425 n. 2 c.p.) fattispecie incriminatrice posta a tutela della pubblica incolumità».

[710] Sull'argomento, si veda, in particolare FLOR, *Data retention ed art. 132 cod. privacy: vexata quaestio (?)*, in *Dir. Pen. Contemp*., 2017, 3.

[711] La prima versione dell'art 132 del Codice *Privacy* risale al d.lgs. 30 giugno 2003, n. 196. Cfr. Cap I § 3.1.

[712] Si fa riferimento al d.lgs. 30 maggio 2008, n. 109 «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». Sul punto v. Cap I § 3.5.

comunitaria. Ciò posto, sarebbe assai arduo sostenere che le pronunce della Corte di Giustizia in materia di *data retention* non abbiano alcun impatto sulla disciplina italiana e, in via mediata, sul procedimento penale in corso. L'unico caso in cui la normativa interna di recepimento potrebbe non risentire della dichiarazione di invalidità della direttiva Frattini[713], sarebbe qualora il legislatore nazionale avesse eliminato in sede di recepimento le criticità dell'atto di diritto derivato[714].

Questo, però, non è il caso dell'Italia. La normativa nazionale in tema di *data retention* non è, infatti, in grado di garantire il rispetto degli *standard* minimi individuati dalla Corte di Lussemburgo, per le ragioni di cui *supra*[715]. Esso osta all'art. 15, par. 1, della direttiva 2002/58/CE, letto alla luce degli artt. 7, 8 e 11 nonché dell'art. 52, par. 1, della Carta di Nizza. Si è, infatti, già visto ampiamente che l'articolo sopracitato «deve essere interpretato nel senso che esso osta ad una normativa nazionale**,** la quale disciplini la protezione e la sicurezza dei dati relativi al traffico e dei dati relativi all'ubicazione, e segnatamente l'accesso delle autorità nazionali competenti ai dati conservati**,** senza limitare, nell'ambito della lotta contro la criminalità, tale accesso alle sole finalità di lotta contro la criminalità grave»[716].

Alla luce delle predette osservazioni, un dato appare incontestabile: l'art. 132 del Codice *Privacy* viola il diritto alla vita privata (art. 7 della Carta di Nizza) nonché il diritto alla protezione dei di carattere personale (art. 8), così come interpretati dalla giurisprudenza della Corte di Giustizia. Siffatto contrasto non può essere certo sanato dai giudici nazionali tramite un *iter* argomentativo scarno e poco convincente, con quello fornito dal Tribunale di Padova[717].

---

[713] Cfr. FLOR, Data retention *ed art. 132 Cod*. privacy: vexata quaestio (?), 356.

[714] Sul punto si veda quanto affermato da dell'Avv. Gen. UE *Pedro Cruz Villalón*, presentate il 12 dicembre 2013, nelle cause riunite C-293/12 e C-594/12, *Digital Rights Ireland e Seitlinger*, *cit.,* punto 157. L'avvocato ha affermato che «la direttiva 2006/24 è invalida per effetto della mancanza di inquadramento sufficiente delle garanzie disciplinanti l'accesso ai dati raccolti e conservati e il loro impiego (qualità della legge), a cui tuttavia può essere stato posto rimedio nell'ambito delle misure di trasposizione adottate dagli Stati membri».

[715] Si rinvia al Cap. III § 3.

[716] Sul punto Corte giust. UE, Gr. Sez., sent. 21 dicembre 2016, *Tele2 Sverige*, *cit.*, punto 112.

[717] Cfr. FLOR, Data retention *ed art. 132 Cod*. privacy: vexata quaestio (?), 356.

4.2 L'interpretazione "restrittiva" della Corte di Cassazione (2019).

Allo stesso modo, poco persuasive sono state le motivazioni addotte dal Giudice di legittimità[718] che, secondo l'orientamento prevalente in giurisprudenza, ha negato l'incompatibilità rispetto al diritto sovranazionale della disciplina prevista dall'art. 132 del Codice *Privacy*. Nel caso di specie, la difesa ha censurato la sentenza parzialmente riformata dalla Corte d'appello di Bologna per due motivi: in primo luogo, l'imputato è stato condannato per traffico di stupefacenti[719] pur essendovi a suo carico una sola prova di natura indiziaria. Mediante l'acquisizione dei tabulati telefonici, infatti, il P.M. è stato in grado di risalire alla "cella telefonica"[720] agganciata dall'imputato nel il lasso di tempo in cui sarebbe avvenuta la cessione di droga. Una volta individuata la posizione geografica dell'apparecchio mobile, gli organi inquirenti hanno, dunque, dedotto la presenza dell'imputato nel *locus commissi delicti*[721].

In secondo luogo, la difesa ha sostenuto che la normativa interna di *data retention* non superi il vaglio di proporzionalità ai sensi dell'art. 52 della Carta di Nizza in quanto nell'impianto normativo dell'art. 132 si riscontrano «tutti i vizi già individuati dalla Corte di giustizia». In particolare, anche in questo caso, si è sottolineato come il legislatore italiano abbia predisposto la conservazione dei dati per qualsiasi tipologia di reato, senza limitare la portata della norma alle fattispecie di criminalità grave e senza sottoporre l'acquisizione dei tabulati al vaglio di un giudice[722]. Sulla base di siffatte premesse, la difesa ha chiesto «di disapplicare la norma interna e di ritenere la prova acquisita vietata dalla legge e quindi non utilizzabile». In subordine, ha fatto istanza al Giudice di legittimità di sospendere il procedimento penale in corso e di presentare un rinvio pregiudiziale alla Corte di

[718] Si tratta della Cass. Pen., sez. III, sent. 23 agosto 2019, n. 36380, in *Cass. Pen*., 2019, 409.
[719] Nel caso di cui trattasi, la Corte di appello di Bologna, con la sentenza del 21 dicembre 2017, in parziale riforma della sentenza del Tribunale di Ravenna, aveva confermato la condanna inflitta all'imputato per il reato di traffico di stupefacenti *ex* art. 73 del D.P.R. n. 309 1990, T.U. stupefacenti.
[720] Per la definizione di "cella telefonica" si veda Dinacci, *Localizzazione attraverso celle telefoniche*, in AA. VV., *Le indagini atipiche,* Scalfati (a cura di), Torino, 2014, 370.
[721] La tecnica utilizzata dall'Accusa è nota come "*cell site analysis"* e permette di geolocalizzare il dispositivo mobile qualunque attività su di esso sia rilevata. Tra di esse, sono incluse non solo la ricezione o l'effettuazione di chiamate ma anche messaggistica istantanea o connessione ad *Internet*. Per un approfondimento sul punto si rinvia al Cap. I.
[722] Cfr. LUPÀRIA, Data retention *e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, *cit.,* 758.

Giustizia avente ad oggetto la compatibilità delle previsioni nazionali rispetto al diritto comunitario.

Ebbene, la Consulta ha accolto il primo motivo di impugnazione sulla base dell'orientamento consolidato in giurisprudenza[723] secondo cui il riscontro investigativo della presenza del telefono cellulare in una determinata zona, coincidente con il *locus commissi delicti* «può essere qualificato quale indizio, ma di per sé non dimostra nulla, anche se l'utenza è precisamente attribuita ad una determinata persona». Per accertare la colpevolezza dell'imputato al di là di ogni ragionevole dubbio sono necessari «altri indizi, ugualmente gravi e precisi, ed infine tutti concordanti, che possano consentire di affermare che il possessore dell'utenza ha commesso il reato»[724].

In merito al secondo motivo di impugnazione, la Corte di Cassazione ha, invece, rigettato *in toto* le istanze della difesa e ha ritenuto non necessario disporre il rinvio pregiudiziale alla Corte di Giustizia ai sensi dell'art 267 TFUE[725]. A sostegno di siffatta decisione, il collegio si è limitato a riportare le argomentazioni di cui i giudici della Corte si erano fatti portavoce già in precedenza[726], focalizzandosi su due questioni principali. Di seguito, si ripercorrerà in breve l'*iter* argomentativo del Giudice di legittimità.

In primis, la Corte ha affermato che la disciplina attuale del Codice *Privacy* non entrerebbe in contrasto con il diritto comunitario, così come interpretato alla luce delle sentenze *Digital Rights Ireland* e *Tele 2 Sverige,* in quanto queste ultime

---

[723] Sul punto si veda Cass. Pen., Sez. V, Sent., 22 gennaio 2019, n. 2932; Cass. Pen. Sez. I, Sent. 2 maggio 2016, n. 18149; nonché di recente, Cass. Pen. Sez. II, 11 dicembre 2020, n. 35447. Tutte le pronunce sono consultabili *online* su *www.dirittoegiustizia.it.*

[724] Cfr. Cass. Pen., sez. III, sent. 23 agosto 2019, n. 36380, cit., 409, punto 2.4. Inoltre, la Consulta ha ribadito che «In punto di diritto deve infatti affermarsi che l'elemento di prova costituito della presenza di un telefono in una determinata cella dimostra, solo ed esclusivamente, che l'utilizzatore di quel telefono si trova in un data zona: per altro anche piuttosto grande, perché le celle telefoniche non identificano un luogo preciso ma una zona di copertura della rete telefonica di grandezza variabile; nel caso in esame, la grandezza delle celle prese in esame non è neanche indicata: pertanto l'utilizzatore del n. (OMISSIS) e G.D. avrebbero potuto trovarsi anche in due luoghi differenti».

[725] Sul punto, la Corte ha «Anzitutto ricordato che (cfr. Cass. Pen., Sez. IV, 19 luglio 2017, n. 50998) il rinvio pregiudiziale alla Corte di Giustizia Europea ai sensi dell'art. 267 del Trattato sul funzionamento dell'Unione Europea non costituisce un rimedio giuridico obbligatorio, esperibile automaticamente a sola richiesta delle parti, spettando solo al giudice stabilirne la necessità. Nel caso in esame tale necessità non sussiste».

[726] Si veda, in particolare, quanto affermato nella sent. Cass. Pen., sez. V, 24 aprile 2018, n. 33851, in *Cass. pen*., 2019, 299, a cui la Corte rinvia espressamente. Nel caso di specie, la disciplina italiana in tema di acquisizione di dati contenuti nei tabulati telefonici era stata dichiarata compatibile con il diritto sovranazionale come interpretato dalla Corte di Giustizia dell'Unione europea.

sarebbero indirizzate soltanto agli Stati membri privi di normativa interna in tema di *data retention*[727]. Di conseguenza, l'Italia che, mediante l'emanazione del d.lgs. n. 196 del 2003 ha dato attuazione alla direttiva 2002/58/CE, non potrebbe rientrare nel novero dei destinatari delle pronunce della Corte di Giustizia sopracitate.

In secundis, il collegio ha affermato che, in ogni caso, l'art. 132 supererebbe appieno il vaglio di proporzionalità[728] ai sensi dell'art. 52 della Carta di Nizza dedotto dalla difesa. Secondo i giudici, la disciplina interna non solo delimiterebbe in modo efficace il periodo di conservazione dei dati, ma soprattutto subordinerebbe al vaglio di un organo indipendente, il P.M., l'acquisizione dei tabulati in conformità con gli *standard* imposti in ambito comunitario[729]. La contestazione effettuata dal ricorrente si fonderebbe, infatti, su un «errore»[730] nella traduzione in lingua italiana delle sentenze sopracitate, in cui si riporta la frase «un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente»[731].

A detta della Corte, siffatta traduzione non sarebbe «del tutto fedele» alle versioni delle sentenze in lingua inglese e francese, in cui sono rispettivamente adoperati i termini "court"[732] e "juridicion"[733]. In entrambi i casi, infatti, le locuzioni sopracitate sarebbero riferibili alla magistratura intesa come "organo", e cioè composta sia da giudici sia da pubblici ministeri. Di conseguenza, secondo l'interpretazione della Cassazione italiana, la Corte di Lussemburgo avrebbe inteso fare riferimento

[727] Cfr. Cass. Pen., sez. III, sent. 23 agosto 2019, n. 36380, cit., 409, punto 3.5, secondo cui «Quanto all'impatto nel sistema normativo italiano dei principi enunciati con le sentenze della Corte di Giustizia, la Corte di Cassazione ha affermato che tali sentenze hanno riguardato Stati privi di una regolamentazione dell'accesso e della conservazione dei dati, mentre lo Stato italiano si è dotato di una specifica disciplina».
[728] Sul principio di proporzionalità, si rimanda a quanto detto *supra*.
[729] Secondo i Giudici, l'art. 132 del Codice *Privacy* dispone «l'enunciazione della finalità di repressione dei reati; la delimitazione temporale dell'attività di memorizzazione; l'intervento preventivo dell'autorità giudiziaria, funzionale all'effettivo controllo della stretta necessità dell'accesso ai dati, nonchè al rispetto del principio di proporzionalità in concreto».
[730] Cfr. Cass. Pen., sez. III, sent. 23 agosto 2019, n. 36380, *cit.*, 409, punto 3.6.
[731] Cfr. Corte giust. UE, Gr. Sez., sent. 8 aprile 2014, *Digital Rights Ireland*, *cit.*, punto 62; Cfr. Corte giust. UE, Gr. Sez., *Tele2 Sverige*, sent. 21 dicembre 2016, *cit.*, punto 125.
[732] Secondo la Corte, «nella versione inglese delle sentenze viene adottato il termine "Court", anch'esso promiscuo, considerato che la funzione giudiziaria è, in via generale, indicata con la formula "Court clerk", mentre termini precisi designano il giudice (judge) e il pubblico ministero britannico (prosecutor), quest'ultimo privo della prerogativa italiana dell'indipendenza».
[733] «Nella versione francese delle sentenze, è stato adoperato il termine "juridiction", riferibile quindi alla magistratura francese nel suo complesso, composta da giudici e da pubblici ministeri (*magistrats du parquet*)».

all'«autorità giudiziaria» nel suo complesso, in cui sono pacificamente ricompresi gli organi inquirenti.

A sostegno di questa lettura meno garantista, il collegio ha fornito una ulteriore argomentazione che ha visto l'istituto della *data retention* nuovamente a confronto con la disciplina delle intercettazioni, mezzo di ricerca della prova in parte affine[734]. Ebbene, secondo la Suprema Corte, il controllo del pubblico ministero sull'attività di acquisizione dei dati di traffico garantirebbe un adeguato livello di tutela. Sul punto, i giudici hanno, infatti, osservato che l'accesso da parte delle autorità inquirenti ai dati "esterni" alla comunicazione comporti una lesione del diritto alla *privacy* e della segretezza delle comunicazioni (*ex* art. 15 Cost) molto meno intensa a quella realizzata dalle intercettazioni, il cui procedimento è affidato al controllo di un giudice. Secondo l'approccio della Corte, dunque, il fatto che ad autorizzare l'acquisizione dei dati di traffico sia solo il pubblico ministero assicurerebbe un livello adeguato di garanzie, soprattutto a fronte di una compromissione della "sfera privata" inferiore rispetto alle intercettazioni[735].

Anche in questo caso, l'*iter* motivazionale della Corte di Cassazione risulta poco persuasivo e inidoneo a sconfessare l'incompatibilità della disciplina nazionale rispetto ai principi proclamati dalla Corte di Giustizia in tema di *data retention*.

In primo luogo, appare non condivisibile l'argomento preliminare[736] su cui si fonda la pronuncia in esame, in base al quale la Corte afferma che le sentenze *Digital Rights Ireland* e *Tele2 Sverige* dispiegherebbero il loro contenuto prescrittivo soltanto nei confronti degli ordinamenti nazionali mancanti di normativa in tema di *data retention*. Siffatto rilievo risulta *ictu oculi* non conforme alla realtà e denota un vizio metodologico da parte dei giudici italiani. Nella sentenza *Tele 2 Sverige*, la Corte di Giustizia, infatti, ha esaminato le disposizioni svedesi e inglesi in tema di *data retention*, ossia di Paesi tutt'altro che privi di apposita disciplina in materia. Dall'analisi dei singoli ordinamenti, ha poi ricavato una serie di requisiti

[734] Per l'analisi delle differenze e dei punti di contatto tra i due mezzi di ricerca della prova, si rinvia al Cap. I § 5.1.
[735] Tale argomentazione del Giudice di legittimità richiama quanto già affermato dalla Corte Cost., sent. 11 marzo 1993, n. 81, *cit*. Per la critica all'approccio della giurisprudenza secondo cui è ammissibile la tutela graduale delle guarentigie costituzionali e, in particolare, di quella prevista dall'art. 15 Cost., si rinvia al Cap. II.
[736] Sul punto, LUPÀRIA, Data retention *e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, *cit.*, 762.

universalmente validi, a cui ciascuno Stato dovrebbe adeguarsi nella predisposizione di misure di conservazione dei dati di traffico[737]. In base a tali osservazioni, non si comprende in base a quali evidenze la Corte di Cassazione abbia ritenuto l'art. 132 del Codice *Privacy* esente dalla portata applicativa delle pronunce della Corte di Giustizia.

Il secondo argomento addotto dal collegio risulta altrettanto poco convincente. Infatti, il significato ampio che il Giudice di legittimità ha attribuito al vocabolo «giudice», facendolo, di fatto, coincidere quello di «autorità giudiziaria», non sembra coerente rispetto alle scelte lessicali nell'ambito del diritto comunitario. A ben guardare, si rileva che, quando in altri contesti[738] il legislatore dell'Unione abbia voluto riferirsi al concetto di «autorità giudiziaria», non abbia utilizzato le locuzioni "court" e "juridicion", bensì le più ampie espressioni "judicial authority" o "autoritè judiciaire"[739]. Evitando di dilungarsi in una disamina linguistica che sarebbe di ostacolo all'economicità del presente lavoro, risulta abbastanza difficile sostenere che la Corte di Giustizia, nella redazione delle sentenze in esame, non abbia affatto tenuto in considerazione il lessico utilizzato dal legislatore europeo, facendo scelte stilistiche differenti. Ciò posto, l'argomentazione della Consulta risulta poco soddisfacente, perché, seppur non sostenuta da evidenze sufficienti, tende a depotenziare alla radice la portata delle garanzie di tutela imposte dagli artt. 7 e 8 della Carta di Nizza[740].

Inoltre, a privare di ulteriore credibilità la tesi della Corte Cassazione è la sentenza della Corte europea dei diritti dell'uomo *Szabó e Vissy c. Ungheria*[741],

---

[737] Si vedano, in proposito, solo a titolo di esempio, i punti 15 e ss. della sentenza Corte giust. UE, Gr. Sez., *Tele2 Sverige*, sent. 21 dicembre 2016, *cit.*, in cui è descritta la disciplina svedese e poi del Regno Unito in materia di *data retention*. Per un approfondimento sul contenuto di siffatta pronuncia si rimanda al Cap. II.

[738] Si pensi, a titolo meramente esemplificativo, all'art. 6 della decisione quadro 2002/584/ GAI «relativa al mandato d'arresto europeo e alle procedure di consegna tra Stati membri». Nella norma sopra richiamata, si fa riferimento all'autorità giudiziaria dello Stato membro competente ad emettere il c.d. MAE. Per visualizzare le traduzioni in lingua italiana, inglese e francese e mettere a confronto le scelte lessicali del legislatore europeo, si rinvia a *www.eur-lex.europa.eu*.

[739] La traduzione di siffatte espressioni in lingua inglese e francese è perfettamente coincidente con il concetto di «autorità giudiziaria» dell'ordinamento italiano. Per un approfondimento sull'argomento, si rinvia a GUARNIERI, *Lineamenti di diritto comparato*, Milano, 2020.

[740] Sul punto, LUPÀRIA, Data retention *e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, *cit.*, 762; MARCOLINI, *L'istituto della* data retention *dopo la sentenza della corte di giustizia del 2014*, *cit.*, 1594.

[741] Si fa riferimento alla sent. Corte EDU, 12 gennaio 2016, sez. IV, *Szabó e Vissy c. Ungheria,* punto 77, disponibile *online www.hudoc.echr.coe.int.* Nel caso di specie, si è trattato il tema della sorveglianza segreta alla luce delle nuove tecnologie. Per un approfondimento sull'evoluzione della giurisprudenza della Corte di giustizia dell'Unione europea in materia, si rimanda a SEMINARA, *Sorveglianza segreta e nuove tecnologie nel diritto europeo dei diritti umani,* in *Medialaws – Rivista dir. media*, 2017, 133 e ss.

richiamata nel caso *Tele2 Sverige*. In siffatta pronuncia, i giudici di Strasburgo, pur ammettendo che anche le autorità indipendenti possano predisporre limitazioni al diritto alla riservatezza, hanno affermato che «il controllo del giudice offre le migliori garanzia di indipendenza e imparzialità». Si è, dunque, manifestato un espresso *favor* circa la necessità di che le limitazioni della *privacy* del singolo siano sottoposte al controllo preventivo di una "court". Ciò posto, risulta arduo ritenere che la Corte di Giustizia abbia voluto estendere anche alla figura dei pubblici ministeri il potere di autorizzare l'attività acquisitiva dei dati di traffico.

Da tali osservazioni, si deduce che a livello comunitario[742] si sia affermata la necessità di sottoporre al vaglio di un organo non soltanto indipendente, bensì anche terzo ed imparziale[743], l'accesso ai tabulati telefonici e telematici. Soltanto il rispetto di un requisito così stringente è, infatti, in grado di assicurare la tutela dei diritti fondamentali previsti dagli artt. 7 e 8 della Carta di Nizza. A nulla rileva, che mediante l'istituto della *data retention* si acquisiscano dati "esterni" che non includono il "contenuto" dell'atto comunicativo[744], al contrario delle intercettazioni. Nelle pronunce sopra citate, i giudici della Corte di Lussemburgo, infatti, hanno sottolineato che le ingerenze nella "sfera privata" del singolo causate dalla conservazione e dall'acquisizione dei dati di traffico siano potenzialmente «gravi»[745]. Orbene, proprio

---

[742] Sul punto, si veda sent. Corte giust. UE, Gr. Sez., *Tele2 Sverige*, sent. 21 dicembre 2016, *cit.* punto 123. Più diffusamente, come si è già visto nel Cap. II, la necessità di affidare ad un organo terzo ed imparziale il controllo preventivo sull'accesso ai dati di traffico è stato ribadito Corte giust. UE, Gr. Sez., sent. 2 marzo 2021, *H.K. Danmark, cit.*, punto 54. In siffatta pronuncia, i giudici hanno ritenuto opportuno che «tale autorità abbia la qualità di terzo rispetto a quella che chiede l'accesso ai dati, di modo che la prima sia in grado di esercitare tale controllo in modo obiettivo e imparziale al riparo da qualsiasi influenza esterna. In particolare, in ambito penale, il requisito di indipendenza implica, come rilevato in sostanza dall'avvocato generale al paragrafo 126 delle sue conclusioni, che l'autorità incaricata di tale controllo preventivo, da un lato, non sia coinvolta nella conduzione dell'indagine penale di cui trattasi e, dall'altro, abbia una posizione di neutralità nei confronti delle parti del procedimento penale».

[743] Nell'ordinamento processuale italiano, il principio della «imparzialità» impone che non vi siano legami tra il giudice e le parti. La «terzietà» si riferisce, invece, allo *status* dell'organo giurisdizionale e al ruolo "neutrale" che svolge all'interno del processo. In dottrina, quest'ultima è stata interpretata come un limite al passaggio tra le funzioni di P.M. e quelle di giudice e viceversa. Sul punto, v. FERRUA, *Il "giusto processo" in Costituzione*, in *Dir. giust.*, 2000, n.1, 78; FRIGO, *Così le scelte sulla valutazione delle prove vanificano le conquiste sul giusto processo*, in *Guida Dir*., 1999, 48.

[744] Per un approfondimento sul punto, si rinvia al Cap. II.

[745] Sul punto v. Corte giust. UE, Gr. Sez., sent. 2 marzo 2021, *H.K. Danmark, cit.*, punto 21. Nel caso di specie, i giudici di Lussemburgo hanno affermato che «l'accesso delle autorità nazionali a dati che consentano di identificare la fonte e la destinazione di una comunicazione telefonica a partire dal telefono fisso o mobile di un sospettato, di determinare la data, l'ora, la durata e la natura di tale comunicazione, di identificare le apparecchiature di comunicazione utilizzate, nonché di localizzare il materiale di comunicazione mobile utilizzato, costituisce un'ingerenza nei diritti fondamentali in

in ragione della lesività della *data retention* sulla *privacy* del singolo, a livello comunitario sono stati previsti *standard* di garanzia così elevati.

In definitiva, per le ragioni sopra esaminate, nemmeno le argomentazioni addotte dalla Corte di cassazione risultano idonee a sostenere la tesi secondo cui l'art. 132 del Codice *Privacy* sarebbe compatibile rispetto al diritto comunitario[746]. Davanti ad una simile evidenza, il collegio avrebbe dovuto disapplicare la norma sopracitata e dichiarare inutilizzabili le prove acquisite o, al massimo, sollevare la domanda di rinvio pregiudiziale ai sensi dell'art. 267 TFUE. Qualora sussista un potenziale contrasto tra un atto legislativo interno e l'ordinamento sovranazionale, è, infatti, competenza della Corte di Giustizia pronunciarsi nel merito della questione[747].

Eppure, anche nelle pronunce successive[748], il Giudice di legittimità non si è discostato dalla decisione sopra esaminata, continuando ad escludere il contrasto della disciplina italiana di conservazione dei dati di traffico rispetto al quadro normativo sovranazionale.

---

questione di gravità tale che tale accesso dovrebbe essere limitato alla lotta contro le forme gravi di criminalità, indipendentemente dal periodo per il quale le autorità nazionali hanno richiesto l'accesso ai dati conservati».

[746] In dottrina, l'incompatibilità dell'art. 132 del Codice *Privacy* rispetto al diritto comunitario viene addirittura descritta come "inevitabile". In questo senso, MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale, cit.*, 778. In senso conforme, v. TROGU, *Sorveglianza e "perquisizioni"* on-line *su materiale informatico*, in AA.VV., *Le indagini atipiche*, a cura di SCALFATI (a cura di), Torino, 2014, 441.

[747] I Trattati prevedono una forma di cooperazione giudiziaria tra il giudice dell'Unione e i giudici nazionali, basata sul rispetto delle reciproche sfere di competenza. Mentre ai giudici nazionali compete assicurare l'applicazione del diritto comunitario nell'ordinamento giuridico interno, il controllo sulla legittimità degli atti e l'interpretazione del diritto dell'Unione è di competenza esclusiva della Corte di Giustizia. Ne consegue che «giudice nazionale e Corte di giustizia sono chiamati a contribuire reciprocamente all'elaborazione di una decisione al fine di assicurare l'applicazione uniforme del diritto comunitario nell'insieme degli Stati membri». Sul punto, v. sent. Corte Giust., 1° dicembre 1965, *Schwarze*, in *Raccolta*, 1094.

[748] In particolar modo, si fa riferimento a Cass. Pen., Sent., 25 settembre 2019, n. 48737, in *Cass. Pen*, 2020. Nella pronuncia *de qua*, il Giudice di legittimità afferma che, sebbene la disciplina prevista dall'art. 132 del Codice *Privacy*, non limiti l'attività di conservazione dei dati a reati particolarmente gravi, risulti comunque compatibile con il diritto sovranazionale. Spetterebbe, infatti, al giudice di merito verificare, in concreto, il rapporto di proporzionalità tra «la gravità dell'ingerenza nel diritto fondamentale alla vita privata e quella del reato oggetto di investigazione». Sul punto, v. anche Cass. Pen. Sez. II sent., 10 dicembre 2019, n. 5741, in *Cass. Pen*, 2020. Nel caso di specie, la Consulta ha ritenuto legittimo l'accesso ai dati del traffico telefonico in quanto finalizzato all'accertamento di un delitto di associazione a delinquere, reputato «grave».

4.3 La "svolta" garantista del g.i.p. di Roma: una possibile soluzione.

Il primo segnale di un cambiamento di rotta da parte della giurisprudenza nazionale è rappresentato da un recente provvedimento[749] del g.i.p di Roma, emesso a seguito della sentenza della CGUE *H.K Danmark*[750]. Nel caso di specie, dinanzi alla richiesta di autorizzazione da parte del P.M. a disporre l'accesso dei dati relativi al traffico *ex* art. 132 del Codice *Privacy,* il giudice ha dato la prima applicazione pratica di quanto stabilito nella pronuncia sopracitata[751]. Di seguito, si ripercorrerà il ragionamento da questi sviluppato per capire in che modo si sia giunti a tale approdo esegetico innovativo.

Innanzitutto, nel decreto di cui trattasi, il g.i.p. ha riportato alcune tra le principali argomentazioni dei giudici di Lussemburgo, secondo cui l'attribuzione del controllo preventivo sull'acquisizione dei tabulati spetterebbe soltanto all'organo giurisdizionale, in ragione della neutralità e indipendenza[752] rispetto alle parti all'interno del procedimento penale. Siffatti requisiti sarebbero, infatti, intrinsecamente estranei alla parte pubblica, la quale, in forza della disciplina vigente del codice di rito italiano, può disporre «accertamenti su fatti e circostanze a favore della persona sottoposta alle indagini»[753]. Inoltre, il requisito della terzietà[754], espressamente richiesto dagli *standard* europei, non potrebbe che attribuirsi, per definizione, alla figura del giudice.

In base a tali osservazioni, il g.i.p. ha affermato che la recentissima sentenza *H.K. Danmark* risulti idonea non soltanto a sconfessare i precedenti arresti[755] del Giudice di legittimità, ma soprattutto a ribadire il contrasto tra la disciplina interna e il quadro sovranazionale in materia di c.d. *data retention*. In conseguenza di siffatto conflitto,

---

[749] Si fa riferimento al G.i.p. Roma, decreto 25 aprile 2021, giud. Sabatini. Il documento è disponibile *online* nella sua versione integrale su *www.sistemapenale.it.*

[750] Per l'approfondimento sul contenuto della sentenza si rimanda sempre al Cap. II.

[751] Cfr. DELLA TORRE, *L'acquisizione dei tabulati telefonici nel processo penale dopo la sentenza della Grande Camera della Corte di Giustizia UE, cit.*

[752] In particolar modo, è richiamato espressamente il punto 54 della Corte giust. UE, Gr. Sez., sent. 2 marzo 2021, *H.K. Danmark, cit.*

[753] Cfr. art. 358 c.p.p. rubricato «attività di indagine del pubblico ministero».

[754] In merito al requisito della «terzietà», il giudice ha affermato che la Corte di Giustizia, le ha assegnato un valore «dirimente». Sul significato che tale concetto ha nell'ordinamento italiano si rimanda a quanto detto *supra*.

[755] In particolare, si fa espresso riferimento a Cass. Pen. Sez. II sent., 10 dicembre 2019, n. 5741, *cit*; Cass. Pen., sez. V, 24 aprile 2018, n. 33851, *cit*.

secondo il g.i.p. sarebbe opportuno non applicare[756] la normativa italiana, nel rispetto del principio del primato del diritto comunitario sull'ordinamento normativo interno. In altre parole, l'art 132, comma 3, del Codice *Privacy*, nella parte in cui dispone che il P.M. possa acquisire con decreto i tabulati telefonici e telematici, non dovrebbe produrre più effetti *ex nunc,* essendo necessario, fin da subito, richiedere l'autorizzazione dell'organo giurisdizionale.

Ciò posto, il g.i.p. ha fatto un ulteriore passo in avanti, elaborando una soluzione "creativa"[757] al *vacuum* normativo che verrebbe a crearsi a seguito dell'espulsione dall'ordinamento interno dell'attuale disciplina in materia di dati di traffico. Sul punto, ha riscontrato, infatti, che le «indicazioni della Corte, non altrimenti interpretabili» renderebbero la sentenza sopracitata «direttamente applicabile con effetti vincolanti *erga omnes*». Di conseguenza, essa dovrebbe applicarsi nel nostro ordinamento in luogo della normativa interna non più in vigore, in attesa di un intervento del legislatore in materia.

Inoltre, secondo il g.i.p., non sarebbe di ostacolo alla diretta applicabilità del diritto Ue, così come interpretato dai giudici di Lussemburgo, l'assenza di determinazione in astratto delle «forme gravi di criminalità» in base alle quali è possibile procedere alla conservazione dei dati di traffico. In tal senso, sarebbe possibile ricorrere, per analogia, alla disciplina delle intercettazioni[758] e, in particolar modo, al catalogo dei reati presupposto previsto dagli art. 266 c.p.p. e 266-*bis* c.p.p[759]. In definitiva, secondo il g.i.p., sarebbe possibile sopperire all'indeterminatezza di alcune espressioni contenute

---

[756] Il g.i.p. precisa che, nel caso di specie, «non si tratta pertanto di disapplicazione (perchè ciò evocherebbe vizi della norma statale in realtà insussistenti) bensì della diretta applicazione della prevalente normativa sovranazionale, così come interpretata dalla Corte di giustizia, in conformità al principio della pluralità degli ordinamenti giuridici costantemente applicato (a partire dalla fondamentale sentenza della Corte Costituzionale 8 giugno 1984, n. 170) per la soluzione del conflitto tra norma dell'Unione Europea e norma statale». Per un approfondimento sulla differenza tra "non applicazione" e "disapplicazione" della legge ordinaria, si veda BIN, PITRUZZELLA, *Diritto costituzionale,* Torino, 2020, 450.

[757] Cfr. DELLA TORRE, *L'acquisizione dei tabulati telefonici nel processo penale dopo la sentenza della Grande Camera della Corte di Giustizia UE, cit.*

[758] La proposta del g.i.p. è da apprezzare ancor di più alla luce del fatto che lo stesso Giudice di Legittimità ha, in più occasioni, ribadito «la notevole capacità intrusiva di un'attività investigativa che coinvolga i tabulati» (in tal senso, v. Corte cost., 28 maggio 2010, n. 188, *cit.*), «confermando che, per ogni cittadino, il ricorso a tale strumento d'indagine deve necessariamente essere soggetto alle garanzie previste dall'art. 15 Cost.» (Corte cost., 23 gennaio 2019, n. 38).

[759] Gli articoli del codice di rito penale sopracitati forniscono un elenco tassativo di reati "gravi" per cui è possibile procedere all'intercettazione di conversazioni o comunicazioni telefoniche nonché del flusso relativo a sistemi informatici o telematici.

nella sentenza *H.K. Danmark* attraverso il rinvio integrale a norme a preesistenti all'interno del codice di rito. Ciò eviterebbe che l'autorità giudiziaria italiana non possa più avvalersi uno strumento di fondamentale spesso indispensabile[760] per l'accertamento dei reati, se non a discapito di una sistematica lesione dei diritti fondamentali dell'individuo.

Evitando di entrare nel merito della soluzione pratica offerta dal g.i.p., discutibile sul piano processuale[761], è evidente la portata innovativa del provvedimento in esame. Per la prima volta, un giudice italiano ha rilevato il contrasto tra la disciplina italiana in materia di *data retention* e le fonti comunitarie, sconfessando l'orientamento tradizionale della giurisprudenza nazionale. Inoltre, dopo aver ammesso l'esistenza di siffatto conflitto, ha sostenuto la necessità di dare prevalenza alle fonti sovranazionali, così come interpretate dalla Corte di Giustizia. Di conseguenza, l'art. 132, comma 3, del Codice *Privacy*, nella parte in cui autorizza il pubblico ministero a disporre con decreto di acquisizione, cesserebbe di essere efficace *ex nunc*. Secondo il g.i.p., sarebbe, dunque, necessario, fin da subito, richiedere l'autorizzazione di un giudice per disporre l'acquisizione dei tabulati telefonici, in modo conforme agli *standard* europei.

4.3.1 (Segue) Una lettura alternativa.

A pochi giorni di distanza dall'emanazione del provvedimento appena esaminato, il g.i.p. del tribunale di Roma ha emesso un altro atto[762], per alcuni versi affine al precedente. Anche in questo caso, in risposta all'istanza del P.M. di disporre l'acquisizione dei dati "esterni" alla comunicazione, il giudice ha confermato l'approccio garantista di cui *supra*[763]. Ha, infatti, nuovamente richiamato la sentenza *H.K. Danmark* della Corte di Lussemburgo, sottolineando il contrasto con il

[760] Sull'indispensabilità dell'acquisizione dei dati di traffico per finalità di accertamento e repressione dei reati si rinvia al Cap. I.
[761] Le criticità di siffatta proposta sono state chiaramente rilevate nel successivo provvedimento del g.i.p. di cui seguirà una disamina approfondita.
[762] Si fa riferimento al G.i.p. Roma, decreto 29 aprile 2021, giud. Savio. Il documento è disponibile *online* nella sua versione integrale su *www.sistemapenale.it.*
[763] Sul punto, v. MALACARNE, *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.*, 2021, in *www.sistemapenale.it.*

consolidato orientamento della giurisprudenza italiana di legittimità[764], che reputa conforme agli *standard* europei la disciplina italiana in materia di *data retention*.

Senonché, il g.i.p, a differenza di quanto statuito nel caso precedente, ha ritenuto non fosse possibile procedere alla diretta applicazione del quadro normativo comunitario, così come interpretato dalla Corte di Lussemburgo. Nel provvedimento di cui trattasi si osserva, infatti, che, pur condividendosi il principio secondo cui alle sentenze della CGUE «vada attribuito il valore di ulteriore fonte del diritto comunitario»[765], queste assumono nell'ordinamento interno efficacia immediata e diretta «solo laddove per effetto di tali interpretazioni non residuino negli istituti giuridici regolati concreti problemi applicativi e profili di discrezionalità». Sulla base di tali premesse, il g.i.p. ha constatato che la sentenza *H.K. Danmark* non possa avere efficacia diretta nell'ordinamento nazionale soprattutto a causa della mancanza di precisi riferimenti alle «forme gravi di criminalità», per sopperire alla quale sarebbe necessario «un intervento legislativo volto ad individuare le categorie di reati presupposto per cui dei dati di traffico telefonico e telematico».

Ciò posto, il g.i.p. ha censurato l'approdo esegetico offerto nella precedente pronuncia. Ad avviso del giudicante, infatti, non sarebbe possibile ricorrere per analogia alla disciplina delle intercettazioni e alle categorie di reati tipizzate nell'art. 266 c.p.p. in quanto si tratterebbe di un'elaborazione giurisprudenziale "creativa"[766], volta a sollevare perplessità soprattutto rispetto a quanto affermato nella sentenza *H.K. Danmark*. Sul punto, la Corte di Giustizia ha affermato che la normativa nazionale che disciplina l'accesso delle autorità «deve prevederne le condizioni sostanziali e procedurali»[767]. Inoltre, essa «deve fondarsi su criteri oggettivi per definire le circostanze e le condizioni in presenza delle quali deve essere concesso alle autorità nazionali competenti l'accesso ai dati in questione»[768]. Sarebbe, dunque, la stessa

[764]Anche in questo caso, sono state richiamate espressamente Cass. Pen. Sez. II sent., 10 dicembre 2019, n. 5741, *cit*; Cass. Pen., Sent., 25 settembre 2019, n. 48737; Cass. Pen., sez. V, 24 aprile 2018, n. 33851, *cit*.

[765] Siffatto principio è stato ribadito dalla giurisprudenza di legittimità in Cass. 17 maggio 2019, n. 13425, in *Cass. Pen*., 2020; in tal senso v. anche Cass. Pen. Sez. V, sent. 16 marzo 2012, n. 22577.

[766] Inoltre, secondo il g.i.p., l'elaborazione da parte della giurisprudenza di «criteri del tutto discrezionali» nella determinazione del «catalogo dei reati in relazione ai quali l'autorizzazione può essere concessa» darebbe luogo a variazioni «da sede a sede come è fisiologico che accada nella giurisdizione».

[767] Cfr. Corte giust. UE, Gr. Sez., sent. 2 marzo 2021, *H.K. Danmark, cit*, punto 49.

[768] Cfr. Corte giust. UE, Gr. Sez., sent. 2 marzo 2021, *H.K. Danmark, cit*, punto 50.

pronuncia della Corte di Giustizia ad attribuire alla legge nazionale – e non ai giudici interni – il compito di individuare le modalità, nonché i reati presupposto, per cui è possibile procedere all'acquisizione dei tabulati telefonici[769]. Tale *vacuum* normativo non potrebbe essere risolto mediante il rinvio ad una disciplina preesistente ed estranea all'istituto della *data retention* poiché verrebbe meno la «certezza applicativa» richiesta dalla Corte di Giustizia.

In definitiva, secondo il giudicante, la concreta declinazione dei principi espressi a livello sovranazionale non potrebbe ritenersi demandata all'elaborazione giurisprudenziale ma all'intervento del legislatore, che è tenuto ad adattare la disciplina italiana relativa alla *data retention* alle istanze comunitarie. *In medio tempore*, i giudici non possono attribuire discrezionalmente efficacia diretta alla sentenza della Corte di Giustizia, ma sarebbero tenuti a continuare ad applicare l'art. 132 del Codice *Privacy*. Su tali basi, il g.i.p. dichiara non luogo a provvedere sull'istanza di acquisizione dei dati di traffico e restituisce gli atti al P.M.

Al di là dei differenti approdi argomentativi nelle due pronunce appena esaminate, emerge un dato inconfutabile: la recentissima sentenza della Corte di Giustizia ha avuto nell'ordinamento interno un impatto tale da sconfessare il precedente orientamento della giurisprudenza italiana in materia di *data retention*. Se fino a poco tempo fa, i giudici, sia di merito sia di legittimità, erano fermi nel negare il contrasto tra la disciplina nazionale e gli *standard* europei, attualmente emergono segnali che riflettono un panorama esegetico mutato e più vicino alle istanze comunitarie[770]. La differenza tra i due provvedimenti di cui *supra* concerne, infatti, esclusivamente la diversa modalità – giurisprudenziale o normativa – con cui dare attuazione alle istanze di provenienza comunitaria. Nel primo caso, il g.i.p. ritiene opportuno risolvere il conflitto tra i due ordinamenti mediante la diretta applicabilità della pronuncia dei

[769] Sul punto, il g.i.p. ha affermato che« Ritenuto come nel caso , proprio a partire da tali affermazioni di cui ai punti 49 e 50 , le interpretazioni proposte dalla citata sentenza Corte di Giustizia Unione Europea Grande Sez., Sent., 02/03/2021, n. 746/18 non possano avere effetti applicativi immediati e diretti, per la indeterminatezza , nella sentenza, del riferimento ai casi nei quali i dati di traffico telematico e telefonico possono essere acquisiti , riferimento genericamente operato ai casi di "lotta contro le forme gravi di criminalità" o di "prevenzione di gravi minacce alla sicurezza pubblica" , casi la cui concreta declinazione non può non ritenersi demandata (e venendo di fatto demandata dalla sentenza), in esecuzione ai proposti principi interpretativi della normativa Ue, alla legge nazionale, e non alla elaborazione giurisprudenziale».

[770] Sul punto, MALACARNE, *Ancora sulle ricadute interne della sentenza della Corte di Giustizia in materia di acquisizione di tabulati telefonici, cit.*

giudici europei; nel secondo caso, invece, si attribuisce al legislatore nazionale il compito di declinare l'attuale normativa in materia di conservazione dei tabulati telefonici in modo conforme alle esigenze sovranazionali.

Per conducendo ad esiti interpretativi opposti, questa divergenza non mette, però, in dubbio che l'art. 132 del Codice *Privacy*, almeno nella parte in cui attribuisce il potere di autorizzare l'acquisizione dei dati di traffico al pubblico ministero, violi gli artt., 7, 8 e 52 della Carta di Nizza. Siffatta conclusione, comune ad entrambi i provvedimenti, rappresenta una svolta garantista non indifferente. È, infatti, la prima volta che la giurisprudenza italiana risulti concorde nell'ammettere il contrasto della disciplina nazionale in materia di *data retention e* il quadro normativo comunitario.

4.3 Il rinvio pregiudiziale alla Corte di Giustizia Ue (2021).

La conferma definitiva del tanto atteso *revirement* della giurisprudenza nazionale sull'acquisizione dei dati di traffico nel processo penale proviene dal Tribunale di Rieti[771]. Nel caso di specie[772], i giudici in composizione collegiale hanno sollevato un rinvio pregiudiziale *ex* art. 267 TFUE[773] al fine di verificare la compatibilità tra l'art. 132 del Codice *Privacy* e l'art. 15, paragrafo 1, della direttiva 2002/58/CE[774], così come interpretato dalla Corte di Giustizia. Dopo aver richiamato i principi elaborati dalla CGUE, il collegio ha richiesto una serie di chiarimenti interpretativi al fine di risolvere le problematiche applicative della disciplina italiana sopracitata.

In primo luogo, i giudici remittenti hanno domandato alla Corte di Lussemburgo se l'art. 132, comma 3, del Codice *Privacy*, il quale «renda il pubblico ministero, organo dotato di piene e totali garanzie di indipendenza e autonomia come previsto dalle norme del Titolo IV della Costituzione italiana, competente a disporre, mediante

[771] Si tratta del Tribunale di Rieti, Sezione Penale, Ordinanza, 4 maggio 2021. È possibile consultare *online* la versione integrale del documento su *www.giurisprudenzapenale.com.*

[772] Nel caso di cui trattasi le difese hanno eccepito l'inutilizzabilità processuale dei tabulati telefonici delle utenze in uso agli assistiti alla luce della recente sentenza della Corte di Giustizia Ue *H.K. Danmark*, emessa in data 2 marzo 2021, da ritenersi direttamente applicabile nell'ordinamento interno: in via subordinata, hanno sollevato questione di costituzionalità *ex* artt. 3, 111 e 117 Cost. per contrasto della disciplina nazionale in tale materia con la normativa e i principi omunitari fissati nella detta sentenza. Dinanzi a siffatte eccezioni, il Tribunale, riunitosi in camera di consiglio il 4 maggio 2021 nel procedimento n. 1335/19 RGNR (N. 558/20 RGD) ha sollevato domanda di rinvio pregiudiziale dinanzi alla CGUE.

[773] Per un approfondimento sul rinvio pregiudiziale si rimanda al Cap. II.

[774] L'art. 15 della direttiva è stato riportato integralmente nel Cap. II a cui si rinvia.

decreto motivato, l'acquisizione dei dati relativi al traffico e dei dati relativi all'ubicazione ai fini di un'istruttoria penale debba ritenersi in contrasto rispetto al quadro normativo» europeo. Se, infatti, è possibile assimilare dal punto di vista «funzionale» il P.M. estone[775] e quello italiano, entrambi tenuti a raccogliere prove anche a favore dell'indagato e ad esercitare l'azione penale, le due figure risulterebbero differenti sotto altri profili[776]. Il collegio ha, dunque, ritenuto opportuno sottoporre al vaglio della Corte di Giustizia l'annosa questione circa l'idoneità del pubblico ministero, così come disegnato nell'ordinamento italiano, ad assicurare sufficienti «garanzie di giurisdizionalità».

Dalla risposta a tale quesito da parte dei giudici di Lussemburgo, dipende la compatibilità della normativa cristallizzata nel Codice *Privacy* rispetto agli *standard* europei. Soltanto nel caso in cui la Corte si pronunci in senso favorevole, verrebbero meno tutte le problematiche circa la modalità di adeguamento della disciplina nazionale relativa alla *data retention* alle garanzie processuali rilevate in ambito comunitario. Laddove, invece, la valutazione della Corte dia esito negativo, come è più probabile che accada, ciò avvalorerebbe in modo definitivo la tesi secondo cui l'art. 132 sopracitato è incompatibile rispetto al quadro normativo comunitario, realizzando la dissoluzione di tutti i contrasti dottrinali e giurisprudenziali sul punto.

In secondo luogo, il collegio si è focalizzato sulle possibili ricadute pratiche che la risposta negativa al primo quesito provocherebbe all'interno del nostro ordinamento. Come si è visto poc'anzi, proprio su tale questione gli approcci esegetici della giurisprudenza hanno dato luogo a soluzioni opposte[777]. Il Tribunale di Rieti ha, dunque, ritenuto opportuno sollevare la questione direttamente dinanzi alla Corte di Giustizia. In particolare, il collegio ha chiesto se i principi stabiliti nella sentenza *H.K. Danmark* possano dare luogo all'applicazione immediata all'interno dell'ordinamento

---

[775] Il collegio ha richiamato espressamente il profilo esaminato dalla CGUE nella sentenza *H.K. Danmark* del 2 marzo 2021, punto 14, laddove ha ripreso la "*Legge relativa al pubblico ministero*" estone e in particolar l'art. 1, secondo cui "*Il pubblico ministero è un'autorità soggetta alla sfera di competenza del Ministero della Giustizia*".

[776] Sul punto, il Tribunale sottolinea che «mentre il Pubblico Ministero estone è, appunto, organo di nomina governativa, "soggetto" alla sfera di attribuzioni del Ministero della Giustizia, (v. *Prosecutor's Office Act - Passed 22.04.1998, RT I 1998, 41, 625, Entry into force 20.05.1998, partially 01.01.2001, Art. 1: "Prosecutor's office: The prosecutor's office is a government agency within the area of government of the Ministry of Justice"*), l'organo dell'accusa italiano è, al contrario, assistito da numerose garanzie di autonomia e indipendenza già nella fase "genetica" dell'immissione nell'incarico e non solo nell'esercizio della funzione».

[777] Cfr. Cap II § 4.3 e 4.3.1.

normativo nazionale o se, invece, manchino di «coordinate procedurali e intertemporali che ne impediscano l'efficacia diretta». Soltanto nel primo caso, le norme Ue, così come interpretate dalla Corte di Giustizia, risulterebbero immediatamente operative nell'ordinamento interno, a prescindere da qualsiasi intervento normativo da parte del legislatore.

In alternativa, i giudici remittenti hanno sottoposto alla Corte la questione circa la possibilità «modulare gli effetti della sentenza in chiave retroattiva» al fine di non pregiudicare le esigenze di indagine e di accertamento dei reati nei procedimenti pendenti[778]. Il diritto Ue verrebbe, dunque, direttamente applicato in luogo della disciplina cristallizzata dal Codice Privacy, ma soltanto a partire dai procedimenti penali avviati successivamente alla sentenza del 2 marzo 2021. Tale soluzione, definita come «eccezionale»[779], terrebbe in considerazione della innovatività della posizione della giurisprudenza della CGUE e consentirebbe allo stesso tempo al legislatore nazione di intervenire in materia. Inoltre

Una volta evidenziati i punti essenziali del provvedimento *de quo*, è opportuno fare alcune osservazioni. È evidente che l'ordinanza del Tribunale di Rieti rappresenta l'approdo definitivo dell'annoso dibattito circa il tema della *data retention*. L'ordinanza emessa dal collegio ha, infatti, il pregio di racchiudere in sé, tutti i nodi essenziali che da anni attanagliano dottrina e giurisprudenza nazionale. I giudici non si sono, infatti, limitati a sottoporre al vaglio della Corte di Giustizia la questione circa la compatibilità rispetto al diritto Ue della normativa nazionale, allo stesso modo di altri Stati membri[780], ma hanno richiesto delucidazioni interpretative in merito alle ricadute pratiche che le conclusioni innovative della CGUE realizzino all'interno degli ordinamenti nazionali.

Mentre ai giudici nazionali compete assicurare l'applicazione del diritto comunitario nell'ordinamento giuridico interno, l'interpretazione del diritto

[778] Sul punto, il Tribunale ha affermato che l'idea di «modulare gli effetti della sentenza in chiave irretroattiva» eviterebbe di «pregiudicare fondamentali esigenze di certezza del diritto e "certezza investigativa", limitatamente ai giudizi tuttora pendenti, in chiave di prevenzione e repressione di gravi reati, nell'ottica anche di consentire un possibile e auspicabile intervento del legislatore nazionale in materia senza che si realizzino ingiustificate disparità di trattamento con altri istituti della legislazione nazionale, ad esempio in tema di intercettazioni telefoniche».

[779] Siffatta soluzione è stata già adottata in passato. Sul punto, v. Corte giust. UE, sent. 27 marzo 1980, Vasanelli, *in www.eur-lex.europa.eu.*

[780] Cfr. Corte giust. UE, Gr. Sez., sent. 21 dicembre 2016, *Tele2 Sverige*, *cit;* Corte giust. UE, sent. 2 ottobre 2018, *Ministerio Fiscal*, *cit*.

dell'Unione è di competenza esclusiva della Corte di Giustizia. Nel rispetto di siffatto principio di cooperazione giudiziaria[781], non può essere, rimessa ai tribunali degli Stati membri la valutazione circa la diretta applicabilità del diritto Ue né degli arresti giurisprudenziali dei giudici di Lussemburgo. Spetterebbe, dunque, a questi ultimi – *rectius*, al legislatore europeo[782] – determinare le conseguenze applicative delle loro pronunce, a cui i paesi membri debbono conformarsi.

In attesa di siffatte delucidazioni da parte della Corte di Giustizia, che daranno una risposta definitiva ai quesiti sopra esaminati, l'acquisizione dei dati di traffico per finalità di accertamento dei reati continuerà ad essere oggetto di un cospicuo dibattito dottrinale e giurisprudenziale. Con tutta probabilità, le divergenze sul tema che, fin qui, hanno condotto ad esiti interpretativi opposti in relazione alla possibilità riconoscere efficacia diretta al diritto Ue, continueranno a proliferarsi mettendo in serio pericolo la "certezza del diritto"[783]. L'unica possibilità che si venga a capo della questione già prima della decisione della Corte di Giustizia, sarebbe mediante il tanto atteso intervento legislatore. Soltanto in prospettiva *de jure condendo* sarebbe, infatti, possibile risolvere i contrasti e le incongruenze evidenziate in materia di *data retention* una volta per tutte.

[781] Sul principio di cooperazione giudiziaria e sulla ripartizione delle competenze tra la CGUE e i giudici nazionali si veda quanto detto *supra*.

[782] L'intervento del legislatore europeo è stato più volte sottolineato come auspicale dalla dottrina, soprattutto a seguito della abrogazione della direttiva 2006/24/CE. *Ex multis*, veda FLOR, *La Corte di giustizia considera la direttiva europea 2006/24 sulla cd.* "data retention" *contraria ai diritti fondamentali*, *cit.*, 188. Sul punto, è da segnalare ai lettori che dopo un lungo *iter* di quattro anni, il Regolamento *e-Privacy* ha ottenuto dal Consiglio UE parere favorevole sulla versione finale del testo, con un mandato negoziale per la revisione definitiva. L'entrata in vigore di siffatto Regolamento potrebbe, dunque, cambiare l'assetto normativo comunitario in materia di *data retention*. Per consultare *online* Proposta di Regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche), si veda *www.eur-lex.europa.eu.*

[783] Sul punto è opportuno segnalare un recente provvedimento del Tribunale di Milano che, nel rigettare l'eccezione difensiva di inutilizzabilità dei tabulati telefonici, si è discostato dall'atteggiamento "garantista" dei decreti del g.i.p. di Roma, poc'anzi esaminati. Ciò a riprova che si è ancora ben lontani dal consolidamento dell'orientamento giurisprudenziale che riconosce il contrasto tra la disciplina cristallizzata nel Codice *Privacy*. Si fa qui riferimento al Trib. Milano, VII Sez. penale, ord. 22 aprile 2021, Pres. Malatesta, che è possibile consultare *online* su *www.sistemapenale.it*

SEZIONE II

"*Data retention*" e processo penale

5. Osservazioni preliminari.

Fin qui, la presente ricerca ha adottato un angolo visuale di ampio respiro, privilegiando un inquadramento dell'istituto della *data retention* che tenga in grande considerazione gli interventi normativi e giurisprudenziali di provenienza comunitaria. D'altronde, non si sarebbe potuto fare altrimenti. Si è visto, infatti, come la protezione dei dati e la tutela della *privacy*, valori profondamente incisi dall'acquisizione dei dati di traffico nel procedimento penale, sia – ormai da tempo[784] – una materia di piena competenza dell'Unione europea. In tal senso, si è ritenuto opportuno, dapprima approfondire gli arresti giurisprudenziali della Corte di Giustizia Ue, con cui sono stati ridefiniti gli *standard* di tutela di siffatti diritti[785]; in un secondo tempo, analizzare le conseguenze dirette di tale approccio "garantista" all'interno dell'ordinamento nazionale. Si è, dunque, concluso, che la disciplina italiana attualmente vigente in materia di conservazione dei dati di traffico presenti non pochi punti di frizione rispetto al diritto Ue.

Ebbene, in tale sede è opportuno esaminare la disciplina italiana della conservazione dei dati "esterni" alla comunicazione da un'altra prospettiva, non meno importante. Come si è visto, l'istituto in esame è assimilabile ad un mezzo di ricerca della prova "atipico". Non si potrebbero, infatti, ricavare indicazioni di segno contrario dalla circostanza che la disciplina che regola la conservazione dei dati di traffico sia contenuta nel Codice *Privacy* e non in quello di rito penale. Tale criticabile[786] collocazione non risulta, però, idonea a sottrarre tale istituto ai principi fondamentali che governano la materia.

---

[784] Si faccia riferimento alla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, «relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati», che aveva portato il legislatore interno ad emanare le note leggi n. 675 e 676 del 1996. Per un approfondimento sul quadro normativo in materia di protezione dei dati personali v. Cap. II § 7.

[785] Cfr. Cap II.

[786] In tal senso v. IOVENE, Data retention *tra passato e futuro. Ma quale presente?* 4274. In senso analogo, RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico*, *cit.*, 183.

La disamina che seguirà, avente ad oggetto alcuni tra i diritti processuali previsti nel nostro ordinamento, non ha pretesa di completezza, bensì ha l'obiettivo di evidenziare le incongruenze esistenti tra la tutela di siffatti principi e l'istituto della c.d. *data retention,* così come cristallizzato nel Codice *Privacy*. Al termine della stessa, si sarà in grado di valutare se l'interesse collettivo al perseguimento dei reati e al mantenimento della pubblica sicurezza sia in grado di giustificare le ingerenze che la suddetta normativa realizzi su una serie di prerogative processuali. In caso contrario, sarà opportuno che il tanto auspicato[787] intervento del legislatore in materia sia indirizzato non soltanto ad eliminare i punti di frizione tra l'art. 132 del Codice *Privacy* e il diritto Ue, ma anche le incongruenze rispetto ai principi che governano il diritto processuale italiano. Proprio in tale prospettiva *de jure condendo,* si procede all'analisi di cui *infra*.

6. L'inviolabilità del diritto alla difesa ai sensi dell'art. 24 Cost.

Uno dei valori fondamentali in ambito processuale è il diritto di difesa previsto dall'art. 24, comma 2[788] Cost., che ne "riconosce"[789] l'inviolabilità in ogni stato e grado del procedimento. In generale, si può definire "difesa" la tutela che l'ordinamento accorda al soggetto i cui i diritti vengono compromessi nel corso di una procedura giudiziaria. In particolare, la "difesa penale" è, invece, quella forma di tutela che consente all'imputato di ottenere il riconoscimento della sua innocenza o di ricevere una sentenza di condanna non più grave di quanto sia previsto dalla legge[790].

[787] Sul punto si rimanda a quanto detto *supra.*
[788] L'art 24, comma 2, Cost., prevede che «La difesa è diritto inviolabile in ogni stato e grado del procedimento».
[789] Nel senso che la Costituzione "riconosce" (art. 2 Cost.) e non conia *ex novo* i diritti inviolabili in quanto preesistenti allo stesso ordinamento giuridico. Sul punto, si veda SILVESTRI, *L'individuazione dei diritti della persona*, in *Dir. pen. Cont.*, 2018, 21.
[790] Cfr. TONINI, *Manuale di procedura penale*, *cit.*, 142.

L'enunciato costituzionale summenzionato è stato giudicato "contenutisticamente vuoto"[791] in quanto, una volta enunciata l'inviolabilità[792] della difesa, non viene chiarita l'essenza del diritto e le garanzie procedurali volte a garantirne la sua attuazione concreta[793]. A tal proposito, gli interventi della giurisprudenza hanno giocato un ruolo fondamentale, contribuendo gradualmente ad individuare la struttura e gli strumenti idonei a garantire il diritto di difesa[794].

In primo luogo, la Corte costituzionale[795] ha evidenziato che siffatto precetto trova attuazione all'interno del procedimento penale in una duplice accezione: da un lato viene garantito alla parte il diritto di godere in giudizio dell'assistenza di un esercente la professione legale (c.d. "difesa tecnica")[796]; dall'altra, si assicura all'imputato la possibilità di far valere le proprie ragioni (c.d. "autodifesa") davanti ad un giudice terzo ed imparziale[797]. Sebbene distinte, le due dimensioni del diritto previsto dall'art. 24, comma 2, Cost., non costituiscono due entità autonome in quanto l'aspetto tecnico[798] risulta indispensabile a garantire una concreta attuazione di quello

---

[791] L'espressione è di PANSINI, *Diritto di difesa*, in AA. VV. *Diritti della persona e nuove sfide del processo penale. Atti del XXXII convegno nazionale* (Salerno, 25-27 ottobre 2018), Milano, 2019, 277. L'Autrice ha sottolineato che la garanzia contenuta nell'art. 24, comma 2, Cost., sia «priva di paradigmi quanto all'attuazione» soprattutto se paragonata con i parametri espressi nelle carte internazionali, tra cui l'art. 14 del Patto internazionale relativo ai diritti civili e politici e l'art 6 CEDU. In particolare, quest'ultima norma, oltre ad enunciare l'inviolabilità del diritto alla difesa, assicura che l'accusato riceva un'informativa dettagliata in merito al fatto di reato, che si garantito il tempo necessario per la preparazione della difesa e che sia garantita la facoltà di presenziare al dibattimento. Per un approfondimento sul punto si veda VOENA, *Difesa penale*, in *Enc. Giur. Treccani*, vol X, Roma, 1988.

[792] A differenza di altri diritti "inviolabili" (si vedano ad esempio gli art. 14 e 15 Cost.), la Costituzione non. Prevede la possibilità di eccezionali restrizioni a siffatto diritto. L'"inviolabilità" della difesa è, dunque, da intendersi in senso assoluto. Sul punto, CASELLA, *Sul valore probatorio del contegno non collaborativo dell'imputato nell'accertamento del fatto proprio*, in *Questione Giustizia*, 2.

[793] La formula ampia dell'art. 24, comma 2, era stata pensata per non divenire obsoleta nei decenni successivi a fronte di evoluzioni culturali e per garantire al legislatore discrezionalità nell'attuazione concreta di tale libertà. In dottrina, si veda in tal senso PANSINI, *Diritto di difesa*, in AA. VV. *Diritti della persona e nuove sfide del processo penale., cit.*, 278.

[794] Per una ricostruzione dell'*iter* giurisprudenziale della Corte Costituzionale in materia di diritto di diritto di difesa v. SCELLA, *Per una storia costituzionale del diritto di difesa: la Corte e l'ambiguità del processo "misto"*, In *Il diritto processuale penale nella giurisprudenza costituzionale*, Napoli, 2006, 197 e ss.

[795] Sul punto. v. sent Corte cost. 9 giugno 1961, n. 30, disponibile *online* su *www.giurcost.org*; analogamente, sent. Corte cost. 18 marzo 1957, n. 57, su *www.giurcost.org*.

[796] Sull'argomento v. anche FERRUA, *Difesa (Diritto di)*, in Dig. Pen., 3, Torino, 1998, 466.

[797] In dottrina, nel senso che la composizione degli organi giudicanti che ne pregiudichi l'indipendenza e l'autonomia può a sua volta incidere sull'effettività della difesa. In tal senso, COMOGLIO, *Art. 24, 3° co.*, in *Comm. Cost. Branca*, Bologna-Roma, 1981, 1.

[798] La Corte costituzionale ha sottolineato con forza il fondamentale ruolo che, all'interno del processo, assume la "difesa tecnica", affermando che l'art. 24, 2° co., implica la «*potestà effettiva dell'assistenza tecnica e professionale nello svolgimento di qualsiasi processo, in modo che venga assicurato il contraddittorio e venga meno ogni ostacolo a far valere le ragioni delle parti*». Cfr. sent. C. cost. C. cost. 18 marzo 1957, n. 57, *cit*.

sostanziale. Del resto, la difesa del professionista[799] verrebbe ridotta a mera prerogativa *pro forma* se non fossero di fatto attribuiti alla parte reali poteri di partecipazione per l'enunciazione delle proprie ragioni[800].

Pertanto, la giurisprudenza ha individuato una serie di precondizioni che garantiscano l'effettività dell'esercizio dei poteri difensivi all'imputato e al suo procuratore. In *primis*, è necessario che sia assicurata alla parte il diritto di partecipazione al processo. L'inviolabilità della difesa risulta, infatti, connessa in modo indissolubile al diritto di azione sancito all'art. 24, comma 1, della Cost., secondo cui è necessario garantire all'individuo la tutela giurisdizionale dei propri diritti soggettivi e interessi legittimi. Tale partecipazione deve svolgersi secondo il rispetto del principio di uguaglianza a meno che «non ostino gravi motivi razionalmente giustificabili con il pubblico interesse».[801]

Il secondo presupposto del diritto di difesa consiste, dunque, nel principio del contraddittorio, il quale presuppone l'instaurarsi di un rapporto dialettico tra le parti che interloquiscono in condizioni di parità davanti ad un giudice terzo e imparziale[802]. Viene, così, a crearsi «quel gioco di interventi alternati o contestuali, in quell'andirivieni di domande e repliche, di asserzioni e negazioni»[803] sugli elementi che costituiranno oggetto di decisione del giudice con l'obiettivo che questa verrà emanata sulla base di temi discussi dalle parti[804]. Da tale assunto deriva la necessità che l'interessato sia posto in grado di conoscere tempestivamente gli atti processuali e dedurre prove dei fatti dedotti in giudizio[805].

---

[799] Il difensore è un professionista dotato di specifiche competenze tecnico-giuridiche in ambito penale e civile. Mediante l'atto di conferimento dell'incarico di rappresentanza tecnica, il difensore acquisisce il potere di compiere atti processuali "per conto" e cioè nell'interesse della parte. Per un approfondimento sul tema si veda, TONINI, *Manuale di procedura penale*, *cit.*, 142.
[800] Cfr. COMOGLIO, *Art. 24, 3° co.*, *cit.*, 1.
[801] Così Corte cost. 9 gennaio 1974, n. 2. Nello stesso senso, v. anche Corte cost. 10 febbraio 1972. Entrambe sono disponibili *online* su *www.cortecostituzionale.it.*
[802] Sul punto, v. FERRUA, *Difesa (Diritto di)*, *cit.*, 466.
[803] Si esprime così FERRUA, *Difesa (Diritto di)*, *cit.*, 466.
[804] Sul punto, si veda Corte cost. (ord.) 3 aprile 2000, n. 95 in *www.giurcost.org.*
[805] A tal proposito v. Corte cost. 22 marzo 1971, n. 55, in *www.giurcost.org.*

7. Il diritto alla parità delle armi nel corso del procedimento penale.

La terza e ultima condizione che mira a garantire l'efficacia del diritto di difesa va, dunque, identificata con il diritto alla parità delle armi[806] nel corso del giudizio. In tal senso, l'ordinamento accorda ad entrambe le parti la disponibilità di mezzi di ricerca della prova e ulteriori strumenti tecnico-processuali idonei a condizionare in proprio favore il convincimento del giudice. In ambito penale, la c.d. *egalitè des armes*[807] deve essere, però, coordinata secondo il principio di ragionevolezza[808] con esigenze processuali che possono giustificare un'asimmetria di poteri tra pubblico ministero e difesa[809]. In questo caso, la parità delle parti non presuppone la loro uguaglianza "formale" dinnanzi al giudice, ma impone che ne sia assicurata l'identità "sostanziale" che di fatto garantisca un pari trattamento nella definizione del giudizio.

Proprio alla luce di siffatto principio, è opportuno analizzare la disciplina della c.d. *data retention,* cristallizzata nell'art. 132 del Codice *Privacy*.

Come si è anticipato nel primo capitolo[810], i dati di traffico archiviati dai *service providers* possono essere acquisiti sia dal pubblico ministero, sia dal difensore dell'imputato e dell'indagato[811]. Evitando di ripetersi, in tale sede è opportuno ricordare alcune differenze esistenti tra i due *iter* di acquisizione, con l'obiettivo di verificare se sia effettivamente garantita la parità delle armi tra le parti coinvolte nel procedimento penale. Nel primo caso, il P.M. può procedere mediante decreto motivato, *ex officio* o su istanza di parte, all'apprensione dei tabulati telefonici o telematici di qualsiasi persona coinvolta nel procedimento penale. Qualora invece la richiesta di acquisizione al gestore dei servizi di comunicazione provenga direttamente

---

[806] Siffatto principio è stato enunciato anche a livello sovranazionale dalla Corte EDU, nella sent., 18 marzo 1997, Foucher c. Francia, §34, disponibile *online* su *www.hudoc.echr.coe.int*; vedi anche sent. Corte EDU, 17 luglio 2007, Bobek c. Polonia, § 46. In tali pronunce, la Corte di Strasburgo ha affermato che la parità delle armi, tra accusa e difesa, è una caratteristica imprescindibile di un processo equo. Questa richiede che ad ogni parte sia riconosciuta la possibilità di difendere le proprie ragioni in condizioni che garantiscano una posizione di eguaglianza "sostanziale" rispetto alla controparte.

[807] L'espressione è utilizzata da POLICE, *Commento all'art. 24*, in BIFULCO, CELOTTO, OLIVETTI (a cura di), *Commentario alla Costituzione della Repubblica italiana*, Torino 2006, 502.

[808] Cfr. TONINI, *Manuale di procedura penale*, *cit.*, 230.

[809] Sul punto, si veda Corte Cost. 26 giugno 2009, n. 184, in *www.giurcost.org*. In tale ultima pronuncia, la Corte ha ritenuto giustificata una diseguaglianza in favore dell'imputato «avuto riguardo alle disparità di segno opposto riscontrate durante la fase delle indagini».

[810] Cfr. Cap I §§ 4.3 e 4.4.

[811] V. art. 132, comma 3, del Codice *Privacy*, il cui testo è riportato integralmente nel Cap. I.

dal difensore, questi può limitarsi a richiedere i dati "esterni" alla comunicazione soltanto relativi ad utenze intestate al proprio assistito[812].

Oltre a siffatta censura di natura soggettiva, l'iniziativa istruttoria del procuratore è sottoposta ad un regime differenziato a seconda che la stessa abbia ad oggetto il «traffico in uscita» o il «traffico in entrata»[813]. In breve, nel primo caso, all'istanza del difensore deve essere allegato soltanto l'atto di conferimento dell'incarico professionale, che attesti la legittimazione ad agire del professionista ai dell'art. 391-*quater*[814]. Nel secondo caso, invece, lo stesso ha la possibilità di proporre richiesta di acquisizione dei dati soltanto qualora sia in grado di provare, mediante elementi idonei[815], il «pregiudizio effettivo» alle indagini difensive derivante dal diniego del gestore del servizio adito.

Al di là della ragionevolezza di siffatta distinzione[816], il moltiplicarsi degli adempimenti formali in capo al difensore che richiede l'acquisizione dei dati di «traffico in entrata» è finalizzata soprattutto alla tutela della *privacy* dei "chiamanti" il proprio assistito[817]. Al fine di evitare un potenziale *vulnus*[818] a siffatti soggetti terzi, il difensore è tenuto a giustificare la propria richiesta di acquisizione esibendo al fornitore del servizio di comunicazione adito una serie di atti che documentino, in concreto, il pregiudizio alle investigazioni difensive. Oltre a siffatto pregiudizio, reale e non meramente ipotetico, il richiedente deve attestare il suo interesse ad agire dimostrando la pertinenza dei dati richiesti rispetto al reato per cui si procede. In caso

---

[812] Sul punto, ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, *cit*., 132.

[813] Per la differenza tra «traffico in uscita» e «traffico in entrata» si rinvia al Cap. I.

[814] L'articolo sopracitato si inserisce nel Titolo VI bis interamente dedicato alle investigazioni difensive. Sul punto, v. TONINI, *Manuale di procedura penale*, *cit.*, 666.

[815]Tali presupposti oggetti vi sono stati individuati dal Garante della Privacy con il provvedimento del 3 novembre 2005. Si veda doc. Web n. 1189488 in *www.garanteprivacy.it.*

[816] Cfr. CONTI, *L'attuazione della direttiva Frattini: un bilanciamento insoddisfacente tra riservatezza e diritto alla prova*, *cit.*, 28; CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni,* in *Riv. it. dir. e proc. pen*., 2005, 612. L'Autore afferma che «il ragionamento che ha portato il legislatore a distinguere le chiamate in entrata da quelle in uscita, tutelando le prime più delle seconde, rimane piuttosto misterioso».

[817] Il traffico telefonico in entrata include, infatti, informazioni di carattere personale che riguardano non solo l'utente che riceve la chiamata ma anche tutti gli altri soggetti chiamanti (familiari, colleghi etc. etc.). Ne consegue che l'apprensione di tali dati è suscettibile di ledere non solo la *privacy* del soggetto per cui si procede ma anche quelle di tutti gli altri utenti inevitabilmente coinvolti.

[818]L'espressione è di ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, *cit*., 132.

contrario, il difensore incontrerà il diniego, anche parziale, dell'accesso ai dati di traffico da parte del *service provider*[819].

Sulla base di quanto esposto, è evidente che l'onere motivazionale in capo al difensore, così come inteso dal Garante[820], è assimilabile ad una *probatio diabolica*[821]. Il procuratore che avanza la richiesta di acquisizione *motu proprio* non si limita, infatti, ad attestare la sua legittimazione ad agire ex art. 391-*quater* c.p.p. ma è tenuto a dimostrare quali conseguenze negative deriverebbero dal diniego del gestore dei servizi adito.

Inoltre, l'adempimento da parte del difensore dell'elevata mole di oneri formali potrebbe implicare un rallentamento nelle tempistiche di avanzamento della richiesta di acquisizione dei dati. Come si è già osservato in precedenza, i limiti temporali entro cui è possibile richiedere ai gestori di servizi di comunicazione i tabulati di traffico sono quelli previsti dai commi dai 1 e 1-*bis* dell'art. 132 del Codice *Privacy*. Siffatti termini non sono soggetti a deroghe o proroghe di sorta e, una volta scaduti, i *service providers* sono tenuti alla loro immediata cancellazione. Ciò avviene anche se, nel corso del procedimento giurisdizionale, il procuratore abbia esercitato il diritto di accesso e non abbia ancora ricevuto alcuna risposta da parte del fornitore[822].

Siffatto meccanismo comporta due potenziali rischi che, di fatto, erodono il diritto inviolabile di difesa (*ex* art. 24 Cost.) mediante l'acquisizione di elementi di prova utili alla propria strategia difensiva. In primo luogo, vi è la possibilità che il difensore non riesca a reperire tutti gli elementi utili ai fini della suindicata *probatio diabolica* entro le tempistiche inderogabili previste dall'art. 132 del Codice *Privacy*[823]. In secondo luogo, può accadere che, sebbene il procuratore sia riuscito ad avanzare entro i tempi l'istanza di acquisizione dei tabulati «in entrata», non risulti, comunque, in grado di accedervi per un ritardo nell'elaborazione della risposta da parte dell'operatore telefonico. Come si è affermato poc'anzi, anche qualora la richiesta sia

---

[819] Cfr. Cap I § 4.4.
[820] Si veda doc. Web n. 1189488 in *www.garanteprivacy.it.*
[821] In tali termini si esprime ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, *cit*., 134.
[822] Il carattere stringente del periodo di conservazione dei dati di traffico ai sensi dell'art. 132 del Codice *Privacy* è stato di recente ribadito da Cass. Civ., Sez. I, 28 gennaio 2016, in *www.foro.it*, 2016, 5, con nota di ROSA. L'Autore ha sottolineato che una volta scaduto il termine. Non sussiste l'obbligo di conservazione, anche qualora esso spiri nel corso del procedimento già in atto.
[823] Cfr. FRATTALLONE, *Il trattamento nel processo penale*, in PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, Milano, 2006, 1364.

stata avanzata senza ritardo, la mancata ricezione dei dati entro i tempi preclude al difensore di acquisirli ai sensi dell'art. 391-*quater*.

Sebbene tale ipotesi possa sembrare remota, nella prassi tende a verificarsi con frequenza[824]. All'onere motivazionale aggravato del difensore corrisponde, infatti, un altrettanto complesso vaglio da parte dell'operatore telefonico, il quale è tenuto a svolgere un controllo di merito e non meramente "cartolare"[825]. L'ente privato deve infatti valutare la sussistenza delle condizioni richieste *ex lege* per l'accesso dei dati «in entrata» tra cui, in particolare, il «pregiudizio effettivo». Può dunque accadere che le operazioni necessarie per un simile riscontro siano di particolare complessità causando un rallentamento temporale nell'elaborazione della risposta nei confronti del difensore.

Alla luce di siffatto scenario, è evidente che, nonostante la disciplina prevista dall'art. 132 del Codice *Privacy* riconosca formalmente sia al pubblico ministero sia al difensore dell'indagato il potere di acquisire i dati traffico, non ne garantisce, allo stesso tempo, la c.d. parità dell'armi. In base alle suesposte osservazioni, è emerso, infatti, che l'*iter* aggravato a cui è tenuto il difensore comporti un evidente sacrificio del diritto alla difesa.

8. Il privilegio contro l'autoincriminazione o *right to silence*.

In base alle precedenti osservazioni, è emerso che il diritto inviolabile alla difesa *ex* art. 24, comma 2, Cost, così come inteso dalla giurisprudenza della Corte costituzionale, trova attuazione all'interno del procedimento penale nella duplice accezione di "difesa tecnica" e di "autodifesa"[826]. Ai fini dell'economia del presente lavoro, seguirà un approfondimento soltanto del secondo aspetto, con l'obiettivo di verificare in che modo la normativa italiana in materia di *data retention* si ponga con esso in contrasto.

In via preliminare, è opportuno sottolineare che il diritto di "autodifesa" dell'accusato è un corollario del principio di procedura penale riassumibile con il

[824] Cfr. ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, *cit*., 134.
[825] Sul punto, FRATTALLONE, *Il trattamento nel processo penale*, in PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, *cit.*,1364
[826] Si fa riferimento a quest'ultima componente del diritto di difesa è anche come alla c.d. "difesa personale". Sul punto, si veda CORDERO, *Procedura penale*, Milano, 2003, 285; BELLAVISTA, TRANCHINA, *Lezioni di diritto processuale penale*, Milano, 1987, 244.

brocardo latino *nemo tenetur se detegere* (o *edere*)[827], secondo cui nessuno può essere obbligato ad agire in proprio danno[828]. In senso lato, siffatto principio stabilisce che nessuno può essere obbligato ad affermare la propria responsabilità penale (c.d. auto-incriminazione) o a fornire elementi probatori che concorrano a determinare la propria colpevolezza[829].

A livello sovranazionale, la giurisprudenza della Corte Europea dei Diritti dell'Uomo ha avuto un ruolo decisivo nel tratteggiare il significato[830] e l'ambito di applicazione del principio *nemo tenetur se detegere*[831]. Sebbene privo di espressa menzione nell'art. 6 CEDU[832], la Corte di Strasburgo ha infatti riconosciuto il diritto a non cooperare nell'accertamento penale come uno *standard* internazionale strettamente correlato alla garanzia dell'"equo" processo richiamata nella suddetta

[827] La locuzione è stata elaborata per la prima volta da Thomas Hobbes e recepita nel diritto inglese sin dal XVI secolo, durante l'Illuminismo. Siffatto principio nasce con un valore eminentemente politico e risale all'avversione della classe intellettuale nei confronti dell'*Ancien régime*, il cui assetto istituzionale si fondava sul processo inquisitorio e sulla tortura. In contrapposizione a suddetti valori, si era dunque diffusa l'idea che fosse *contra naturam* ricavare dall'imputato le informazioni necessarie per condannarlo, perché ciò l'avrebbe reso, in un certo senso, "accusatore di se stesso". Sul punto si veda diffusamente, GREVI, «Nemo tenetur se detegere». *Interrogatorio dell'imputato e diritto al silenzio nel processo penale italiano,* Milano, 1972, 7.

[828] In giurisprudenza, la locuzione latina è anche utilizzata nella variante *nemo tenetur se ipsum accusare* che, latamente, può essere tradotta come "nessuno può essere obbligato ad affermare la propria responsabilità penale (auto-incriminazione)". Siffatta espressione ricorre, *inter alios*, nella ordinanza della Corte Costituzionale 10 maggio 2019, n.117, in cui si è recentemente affrontato, con esemplare chiarezza espositiva, la questione dell'ambito operativo del principio in esame. Storicamente limitato soltanto al processo penale, il c.d. diritto al silenzio è stato esteso e adeguato anche ad esigenze di natura amministrativa. È possibile consultare *online* la sentenza sopracitata su *www.giurcost.org*.
In dottrina, sul principio *nemo tenetur se detegere,* si vedano, *ex multis,* MAZZA, *L'interrogatorio e l'esame dell'imputato nel suo procedimento*, *cit*., 45; FERRAJOLI, *Diritto e ragione. Teoria del garantismo penale*, Bari-Roma, 1996, 625.

[829] In dottrina si veda, POLICE, *Commento all'art. 24*, in BIFULCO, CELOTTO, OLIVETTI (a cura di), *Commentario alla Costituzione della Repubblica italiana*, Torino 2006, 502.

[830] A tal proposito, si faccia riferimento alla *Guida all'articolo 6 sul "diritto ad un equo processo"*, elaborata dalla Divisione della Ricerca della Corte Europea del Diritti dell'Uomo e pubblicata nel 2014. Per consultare *online* il testo in lingua italiana si v. *www.echr.coe.int.*

[831] La Corte ha stabilito per la prima volta che le autorità di *law enforcement* non possono obbligare nessuno a cooperare nell'attività di accertamento penale nella sent. Corte EDU, 25 febbraio 1993, Funke c. Francia § 44. In conformità si veda anche sen. Corte EDU, Grande Camera, 25 ottobre 2005, O'Halloran e Francis c. Regno Unito § 45.

[832] L'art. 6 CEDU, par. 1, dispone che «Ogni persona ha diritto a che la sua causa sia esaminata equamente, pubblicamente ed entro un termine ragionevole da un tribunale indipendente e imparziale, costituito per legge, il quale sia chiamato a pronunciarsi sulle controversie sui suoi diritti e doveri di carattere civile o sulla fondatezza di ogni accusa penale formulata nei suoi confronti. La sentenza deve essere resa pubblicamente, ma l'accesso alla sala d'udienza può essere vietato alla stampa e al pubblico durante tutto o parte del processo nell'interesse della morale, dell'ordine pubblico o della sicurezza nazionale in una società democratica, quando lo esigono gli interessi dei minori o la protezione della vita privata delle parti in causa, o, nella misura giudicata strettamente necessaria dal tribunale, quando in circostanze speciali la pubblicità possa portare pregiudizio agli interessi della giustizia».

disposizione. Da tale riconoscimento discendono due corollari: *in primis*, si assicura la tutela dell'accusato rispetto all'impiego di strumenti coercitivi da parte delle autorità che realizzino una compressione della volontà dell'imputato[833]. *In secundis*, la Corte EDU garantisce la facoltà all'imputato di astenersi dal deporre mediante il riconoscimento del c.d. *right to remain silence*[834].

Siffatto principio, così come interpretato a livello sovranazionale[835], trova accoglimento nel nostro ordinamento penale, in primo luogo, nella disciplina relativa all'esame del testimone. Dopo aver enunciato l'obbligo del testimone di rispondere secondo verità alle domande che gli sono rivolte nel corso dell'esame, il codice prende in considerazione il caso in cui, nel replicare a siffatte domande, il testimone possa incolparsi di qualche reato. Davanti ad una situazione simile, se il testimone fosse obbligato a rispondere secondo verità, si troverebbe davanti ad un bivio: rispondere, accusando se stesso, oppure affermare il falso, pur di non riconoscere la propria responsabilità penale. In entrambi i casi, il testimone rischierebbe, però, di essere sottoposto a procedimento penale: nel primo caso, potrebbe subire un'incriminazione per il reato che si è auto-attribuito; nel secondo caso, potrebbe essere indagato per falsa testimonianza[836].

Per evitare il crearsi di siffatto *impasse* giudiziario, il codice riconosce al testimone il diritto a non incriminare se stesso[837], stabilendo che questi non possa «essere obbligato a deporre su fatti da quali potrebbe emergere una sua responsabilità penale»[838]. Viene, così, attribuita al testimone una situazione giuridica soggettiva, assimilabile al "privilegio"[839], che prevede una esenzione dal generale obbligo di

---

[833] Sul punto v. sent. Corte EDU, 17 dicembre 1996, Saunders c. Regno Unito, § 60.
[834] Il diritto a non rispondere fin dal momento in cui l'indagato sia interessato dalla polizia è stato affermato, *inter alios*, nella sent. Corte EDU, 8 febbraio 1996, John Murray c. Regno Unito § 45. Questa e tutte le altre sent. della Corte EDU sopracitate sono reperibili online su *www.hudoc.echr.coe.int.*
[835] In dottrina, per osservazioni a riguardo, si rinvia a EASTON, *Silence and Confessions. The Suspect as the Source of Evidence*, New York, 2014; LAMBERIGTS, *The Privilege Against Self- Incrimination*, *In New Journal of European Criminal Law,* 2016, 42.
[836] V. art 372 c.p.p.
[837] Sul punto, si veda la *Relazione al progetto preliminare e al testo definitivo del codice di procedura penale*, punto 110, secondo cui «il comma 2 dell'articolo 198 è stato modificato per ampliare la tutela contro l'autoincriminazione, non solo a fronte di singole domande, ma, più in generale in relazione a "fatti" suscettibili di generale responsabilità penale».
[838] Cfr. art 198, comma 2, c.p.p.
[839] Nella terminologia anglosassone, il "privilegio" è un interesse privato ritenuto meritevole di tutela dall'ordinamento. Ad esempio, è riconosciuto come "legal privilege" il diritto a mantenere riservate le comunicazioni tra il cliente e il suo consulente professionale. Per approfondimento sul punto, si veda

deporre, qualora dalla risposta su un determinato fatto possa derivarne la responsabilità penale del dichiarante.

In secondo luogo, l'ordinamento riconosce a colui al quale sia stato imputato un fatto di reato il diritto di non concorrere all'accertamento penale fornendo elementi di qualsiasi natura in proprio danno. L'accusato ha, dunque, la facoltà di difendersi tacendo e impedisce che l'eventuale contegno non collaborativo dello stesso possa formare oggetto di valutazione negativa da parte del giudice sotto il profilo probatorio.

Accanto a siffatta dimensione "passiva", la dottrina riconosce una componente "attiva"[840] del diritto di autodifesa secondo cui l'indagato e/o l'imputato ha il diritto di fornire il proprio apporto conoscitivo alla ricostruzione del fatto di reato che gli viene imputato, autodeterminandosi liberamente nelle proprie scelte difensive[841]. In tal senso, viene riconosciuta all'accusato la facoltà di dare un contributo attivo all'accertamento penale, rendendo dichiarazioni inerenti all'illecito da accertare. La più rilevante manifestazione di siffatta facoltà viene rintracciata in istituto processuali quali l'interrogatorio[842], l'esame dibattimentale[843] e in tutti gli altri che prevedono apporti conoscitivi provenienti dall'imputato[844].

In generale, dunque, il diritto di autodifesa riconosciuto dall'ordinamento in capo all'imputato e alla persona sottoposta alle indagini è da intendersi coma libertà

BARLETTA, *Il* "legal privilege" *come principio fondamentale ed i suoi limiti: il caso della normativa antiriciclaggio*, su *www.forumcostituzionale.it*.

[840] Cfr. CASELLA, *Sul valore probatorio del contegno non collaborativo dell'imputato nell'accertamento del fatto proprio*, in *Questione Giustizia*, 1.

[841] Sul punto, v. sent. C. cost. 9 gennaio 1974, n. 2, disponibile *online* su *www.giurcost.org*; analogamente, sent. C. cost. 10 febbraio 1972, n. 27, sempre su *www.giurcost.org*.

[842] Si fa qui riferimento all'interrogatorio dell'indagato disposto dal p.m durante le indagini preliminari e disciplinato dagli artt. 64 e 364 e ss. del c.p.p. Per un approfondimento sull'argomento, si veda MAZZA, *L'interrogatorio e l'esame dell'imputato nel suo procedimento*, Milano, 2004, 45.

[843] L'esame delle parti che ne abbiano fatto richiesta è disciplinato dall'art. 503 c.p.p. Al contrario del testimone, l'imputato non ha l'obbligo di presentarsi (art. 208), né l'obbligo di rispondere alle domande (art. 209, comma 2) né l'obbligo di dire la verità. La distinzione trova conferma nell'art. 197 c.p.p. che dispone l'incompatibilità della qualità di testimone rispetto a quella di imputato. Questo ha luogo non appena è terminata l'assunzione delle prove a carico dell'imputato ai sensi dell'art. 150 disp. att. c.p.p.

[844] In tutti questi casi, l'imputato è considerato "organo" di prova, in quanto titolare di tutta una serie di situazioni giuridiche soggettive "attive". È qualificato, invece, "oggetto" di prova in tutte le situazioni di soggezione, in cui l'imputato viene in rilievo come realtà fisica suscettibile di osservazione. A titolo meramente esemplificativo, si pensi alle indagini effettuate dalla polizia giudiziaria negli accertamenti finalizzati all'identificazione dell'indagato (art. 349, comma 2, c.p.p.), al prelievo di saliva o capelli strumentale (art. 349, comma 2-*bis*, c.p.p.) e ai rilievi ed accertamenti urgenti su persone diverse dall'imputato (art. 354, comma 3, c.p.p.). Per un approfondimento sul punto, v. CAVALLARI, *La capacità dell'imputato*, Milano, 1968, 180; LARONGA, *Le prove atipiche nel processo penale*, Padova, 2002, 55; FELICIONI, *Accertamenti sulla persona e processo penale. Il prelievo di materiale biologico*, Assago, 2007, 33.

di autodeterminazione delle proprie strategie difensive. In base alle precedenti affermazioni, inoltre, è possibile affermare che siffatto diritto sia garantito, in concreto, soltanto qualora sia assicurata all'imputato la prerogativa di fornire alle autorità giudiziarie, soltanto consapevolmente, elementi probatori auto-incriminanti. Difatti, si può dire che soltanto se l'accusato è in grado di conoscere il flusso delle informazioni che lo riguardano e di controllarne l'utilizzo da parte delle autorità inquirenti, allora risulta titolare di un pieno ed effettivo diritto di autodifesa.

In tal senso, la libera determinazione delle informazioni che riguardano la propria personalità all'interno del procedimento penale, o c.d. autodeterminazione informativa[845], risulta essere un corollario applicativo del diritto di autodifesa. Ancor di più, il principio del *nemo tenetur se detegere*, il diritto al silenzio e il diritto a non collaborare con il potere giudiziario risultano tutti collegati da un invisibile *fil rouge* che vede alla sua estremità il diritto alla *privacy*. Una volta accertato che l'istituto del *data retention* comprima quest'ultimo valore[846], allora non dovrebbe destare alcuna sorpresa l'affermazione che l'attività di acquisizione dei dati di traffico da parte dell'autorità giudiziaria interferisca con i valori di natura processuale appena richiamati.

Di seguito, occorre, però, verificare in che modo e con quale intensità l'istituto della *data retention,* così come cristallizzato nel Codice *Privacy,* interferisca con il diritto di autodifesa. In primo luogo, come si è già visto[847], mediante l'apprensione dei dati "esterni" alle comunicazioni, gli organi inquirenti sono in grado di risalire alla localizzazione dell'indagato in un dato momento e di ricostruire il traffico delle chiamate. Tramite tali informazioni relative alla sfera individuale del singolo è possibile, dunque, smentire o confermare le tesi investigative di un soggetto sottoposto alle indagini.

Ciò posto, il fatto che il pubblico ministero possa disporne l'acquisizione senza che l'indagato intestatario dell'utenza telefonica o telematica ne sia informato, nemmeno *ex post*, viola la «sfera» intangibile di autodeterminazione del singolo. Non solo, non è infatti l'imputato a fornire in prima persona elementi probatori che dipendono dalla sua volontà e libertà morale, ma questi non risulta essere nemmeno a

[845] Per un approfondimento sul punto si rimanda al Cap. II.
[846] Cfr. Cap II.
[847] Sul punto, si rinvia al Cap. I.

conoscenza del fatto che sia posta in essere un'attività istruttoria avente ad oggetto l'estrazione dei propri dati personali. Non sa, inoltre, quali siano i dati acquisiti, quale sia il loro contenuto e le informazioni in essi racchiuse e per quanto tempo potranno le autorità inquirenti potranno farne utilizzo.

Ai fini di indagine, l'autorità giudiziaria realizza, dunque, una compressione della libertà positiva di esercitare un controllo sul flusso dei propri dati personali (c.d. autodeterminazione informativa), nella completa ignoranza dell'utente a cui si riferiscono. Inoltre, tramite siffatto mezzo di ricerca della prova, l'indagato, o meglio, «la proiezione integrale della persona nella sua dimensione elettronica»[848] diventa "fonte", o organo[849], di prova, pur non essendone a consapevole. È, infatti, l'accusato stesso che, mediante i dati che forniscono notizie sul proprio traffico telefonico e sulle proprie, fornisce inconsapevolmente elementi idonei a fondare o meno la sua responsabilità penale, per il solo fatto di utilizzare strumenti di comunicazione elettronica. Tali informazioni, contro l'interesse dell'imputato, concorrono a determinarne la colpevolezza nel procedimento penale in corso. Ciò rappresente una violazione del principio *nemo tenetur in se detegere* e del diritto dell'imputato a non collaborare con il potere giudiziario.

Inoltre, il fatto che l'imputato non sia a conoscenza dell'attività istruttoria disposta nei suoi confronti, è di impedimento alla elaborazione di una tesi difensiva efficace. Come si è anticipato[850], uno dei presupposti per il pieno ed effettivo esercizio del diritto di difesa è la partecipazione al processo, che deve svolgersi in condizioni di uguaglianza tra le parti. Siffatta condizione di parità è assicurata, *inter alios*, dal contraddittorio durante la fase dell'assunzione delle prove che garantisce all'interessato la tempestiva conoscenza degli atti processuali e il diritto alla prova circa i fatti su cui si fondano le ragioni della difesa[851]. Soltanto in questo modo, si dà alle parti la concreta «possibilità di tutelare in giudizio le proprie ragioni»[852].

---

[848] Cfr. LUPARIA, *Privacy, diritti della persona e processo penale,* in *Rivista di diritto processuale*, 2019, 1448.
[849] Sul tale argomento v. MARCHETTI, *Testis contra se. L'imputato come fonte di prova nel processo penale dell'età moderna*, Milano, 1994.
[850] Cfr. III §.
[851] Cfr. COMOGLIO, *Art. 24, 3° co.*, *cit.*, 215. Nello stesso senso, in giurisprudenza v. sent, Corte cost., 31 maggio 1996, n. 175, consultabile *online su www.giurcost.org.*
[852]In giurisprudenza, si veda sent. Corte cost. 22 dicembre 1961, n. 70; in conformità, sent. Corte cost. 13 luglio 1963, n. 133. Entrambe le sentenze si possono consultare online su *www.giurcost.org.*

Ciò posto, qualora il pubblico ministero disponga l'acquisizione dei dati di traffico oggetto di conservazione da parte dei *service provider*, non solo non richiede il consenso del soggetto intestatario dell'utenza ma nemmeno provvede ad informarlo. Siffatta carenza sotto il profilo della conoscenza, viola il principio del contraddittorio che non viene nemmeno garantito in differita e non dà la possibilità all'indagato e al suo difensore di adoperarsi nel ricercare la prova contraria. Sebbene si tratti di una considerazione "estensiva" della tutela offerta dall'art. 24 Cost. sarebbe opportuno che il legislatore intervenga a modificare, *de lege ferenda*, i profili di criticità dell'art. 132 Codice *Privacy* appena evidenziati.

9. La presunzione di non colpevolezza.

Un altro principio generale del processo penale che entra in contrasto con la normativa attualmente vigente in materia di *data retention* è la presunzione di non colpevolezza[853]. Siffatto valore è tutelato dall'art. 27, comma 2, della Costituzione ai sensi del quale «l'imputato non è considerato colpevole sino alla condanna definitiva». Anche in questo caso[854], gli interventi esegetici della dottrina e della giurisprudenza hanno contribuito a definire la portata della disposizione costituzionale sopracitata priva di riferimenti procedurali o di attuazione concreta e, a tratti, ritenuta "ambigua"[855].

Secondo l'orientamento prevalente, dalla formula elaborata dall'Assemblea costituente è possibile ricavare due differenti corollari della presunzione di innocenza[856]. In primo luogo, si ritiene che siffatto principio debba essere concepito come la condizione da riservare all'imputato durante tutto il procedimento a suo

[853] In generale, sull'argomento si vedano DOMINIONI, *Imputato*, in *Enc. Dir.,* XX, Milano, 1970, 794; PAULESU, *Presunzione di non colpevolezza,* in *Digesto pen.,* Torino, 1995, 674; ILLUMINATI, *La presunzione di innocenza dell'imputato,* Bologna, 1979.

[854] Si fa qui riferimento all'art. 24, comma 2, che dispone l'inviolabilità del diritto alla difesa. Cfr. Cap. III §.

[855] L'ambiguità della formula adottata dall'art. 27, comma 2, Cost. ha determinato il diffondersi di una lettura alternativa della disposizione in esame. Da parte di alcuni studiosi e della stessa Corte costituzionale (sentenza del 6 luglio 1972, 1974) l'imputato non dovrebbe considerarsi né colpevole né innocente, bensì semplicemente "imputato". Secondo siffatto orientamento minoritario, successivamente smentito dalla Consulta, nessun effetto potrebbe dedursi dalla disposizione costituzionale in materia di giudizio. Sul punto, v. ILLUMINATI, *La presunzione di innocenza dell'imputato,* Bologna, 1979, 28.

[856] Cfr. TONINI, *Manuale di procedura penale*, *cit.*, 253.

carico[857]. Tale "regola di trattamento"[858] fissa, dunque, il divieto a carico del giudice di assimilare l'imputato al colpevole fino a quando non disponga l'emanazione di una sentenza di condanna definitiva[859].

In secondo luogo, l'art. 27, comma 2, detta una regola di giudizio, in stretta connessione con le esigenze processuali di carattere probatorio, secondo cui l'imputato debba essere presunto innocente, fino a quando non emergono elementi probatori che depongano a favore della sua colpevolezza. È possibile, dunque, desumere dall'enunciato costituzionale una presunzione legale relativa[860], e cioè valida fintanto che non sia dimostrato il contrario. Mediante siffatto assunto, l'ordinamento mira ad evitare che l'imputazione assurga a valore assiologico di riferimento a discapito della tesi difensiva di parte[861], e di conseguenza, che il giudice possa orientarsi, nei casi dubbi, sulla colpevolezza dell'imputato. Inoltre, siffatta regola probatoria o di giudizio è meglio precisata nell'art. 6, comma 2, della Convenzione europea dei diritti dell'uomo, ai sensi del quale «ogni persona accusata di un reato è presunta innocente sino a quando la sua colpevolezza non sia stata legalmente accertata».

Una volta delineati gli elementi essenziali di tale principio di diritto penale costituzionale, è opportuno verificare in che modo la normativa italiana in materia di *data retention* interferisca con esso.

Il primo elemento di frizione rispetto al diritto in esame è da individuarsi nel fatto che l'art. 132, comma 1, del Codice *Privacy* preveda una conservazione generalizzata[862] dei dati di dati di traffico telefonico e telematico. Chiunque usufruisca

---

857 In tal senso, D'AMICO, *Commento all'art. 27*, in BIFULCO, CELOTTO, OLIVETTI (a cura di), *Commentario alla Costituzione della Repubblica italiana*, Torino 2006, 556.

858 Ciò, ha portato la giurisprudenza ad elaborare ampie riflessioni sul ruolo della custodia cautelare ai sensi dell'art. 285 c.p.p. In particolare, la Corte costituzionale ha predisposto che le misure di carcerazione preventiva «in nessun caso possono avere la funzione di anticipare la pena da infliggersi solo dopo l'accertamento della colpevolezza». In tal senso, ELIA, *Le misure di prevenzione tra l'art. 13 e l'art. 25 della Costituzione,* in *Giur. cost.,* 1964, 951; AMATO, *Individuo e autorità nella disciplina della libertà personale,* Milano, 1976, 382.

859 Ai sensi dell'art. 656 c.p.p, una sentenza di condanna o di assoluzione risulta "definitiva" o "irrevocabile" quando non può essere più modificata mediante i mezzi di impugnazione ordinari, le cui statuizione sono, perciò, da considerare irrevocabili. Per un approfondimento sul punto, v. TONINI, *Manuale di procedura penale*, *cit.*, 935.

860 Sul concetto di presunzione nel procedimento penale v. CAPOROTUNDO, *Presunzioni legali e onere della prova nel processo penale*, 2017, in *www.giurisprudenzapenale.it.*

861 Cfr. D'AMICO, *Commento all'art. 27*, *cit.*, 556.

862 Sul punto v. CAPUTO, *La conservazione dei dati di traffico telefonico e telematico nella normativa antiterrorismo*, in *Archivio penale*, 2016, n.1, 30. Inoltre, la questione è stata affrontata ampliamente *supra*.

di strumenti di comunicazione elettronica, e, dunque. la quasi totalità della popolazione italiana, è sottoposto a tale operazione di archiviazione da parte dei gestori dei servizi di comunicazione prescelti. Inoltre, come si è già sottolineato[863], siffatta operazione estesa di conservazione dei dati "esterni" è finalizzata non all'accertamento dei reati gravi, ma di qualsiasi reato.

Ciò vuol dire che chiunque comunichi mediante strumenti telefonici o telematici sia, di fatto, "sospettato" di aver commesso qualsiasi fatto di reato ancor prima che questo sia stato commesso. Se è vero, infatti, che è possibile procedere all'acquisizione dei dati "esterni" soltanto una volta avviato il procedimento penale[864], la conservazione degli stessi è disposta a prescindere della ricezione di qualsiasi *notitia criminis*. Ancor prima che l'illecito penale venga ad esistenza e che, di conseguenza, si realizzi la lesione al bene giuridico tutelato dalla norma penale, i *service provider* hanno l'obbligo di porre in essere un'attività finalizzata alla realizzazione di un accertamento penale tutt'altro che certo[865].

L'operazione sopradescritta è sintomatica di una pericolosa tendenza che, negli ultimi anni, si sta riscontrando in ambito processuale. Come si è evidenziato in dottrina[866], si sta gradualmente assistendo al «congedo dall'idea del processo penale come puro luogo d'accertamento di responsabilità per fatti criminosi del passato». In nome della difesa della sicurezza collettiva[867], istanze di repressione penale, classicamente intesa, vengono a mescolarsi con esigenze di prevenzione[868], in un processo di «ibridazione»[869] continua. Non è un caso, dunque, che, anche tramite la

---

[863] Per un approfondimento sul punto si rinvia la Cap. I.
[864] Cfr. art. 132, comma 3, del Codice *Privacy*.
[865] V. LUPARIA, *Privacy, diritti della persona e processo penale,* in *Rivista di diritto processuale*, 2019, 1448.
[866] Sul punto, si veda diffusamente NEGRI, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico),* in *Arch. Pen.*, 2016, n. 1, 44.
[867] Non è un caso che gli atti legislativi che hanno comportato a siffatto mutamento del sistema penale siano stati approvati in prossimità di attentati terroristici o di eventi drammatici che hanno destato preoccupazioni a livello internazionale. In particolare, nell'ambito della normativa del c.d. *data retention*, le principali modifiche della disciplina del Codice *Privacy* sono intervenute dopo gli attentati di Londra e Madrid (d.l. 27 luglio 2005, n. 144) e Parigi (decreto-legge 18 febbraio 2015, n.7). Per un approfondimento sul punto si rinvia al Cap. I.
[868] Sottolineano l'attuale tendenza di mescolare istanze di repressione ad esigenze di prevenzione dei reati ORLANDI, *Relazione introduttiva*, in *Delitto politico e diritto penale del nemico*, GAMBERINI, ORLANDI (a cura di), Bologna, 2007, 35; VIGANÒ, *Terrorismo, guerra e sistema penale*, in *Riv. it. dir. proc. pen*., 2006, 695; nonché ampiamente sul punto, BARTOLI, *Lotta al terrorismo internazionale. Tra diritto penale del nemico*, jus in bello *del criminale e annientamento del nemico assoluto*, Torino, 2008.
[869] L'espressione è di NEGRI, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico)*, *cit.*, *nota 4*.

c.d. *data storage,* l'asse strategico dell'indagine sia stia progressivamente focalizzando verso modalità occulte e atipiche di raccolta di informazioni. Mediante tali strumenti di ricerca della prova, gli organi inquirenti sono in grado di assicurarsi la disponibilità di una serie di elementi probatori che potranno essere successivamente impiegati per l'accertamento penale.

Ciò posto, il compimento in anticipo di attività finalizzate ad un procedimento soltanto eventuale[870] assottiglia la distinzione tra indagini preliminari, il cui avvio coincide con il momento di ricezione della *notitia criminis*[871], e la fase meramente investigativa o delle c.d. investigazioni "proattive"[872]. Il tradizionale confine tra i due momenti distinti viene sostituito da una «zona grigia» in cui le fasi della prevenzione e della repressione diventano «idealmente contigue»[873].

Siffatta tendenza risulta ancora più evidente nella c.d. procedura "di congelamento" (c.d. *quick freeze procedure*)[874] predisposta dai commi 4-*ter*, 4-*quater* e 4-*quiquies*[875] dell'art. 132 del Codice *Privacy*. In sintesi, [876] i commi sopracitati attribuiscono ad un catalogo di soggetti dotati di funzioni esecutive[877] il potere di

---

[870] Così MELILLO, *L'acquisizione dei tabulati relativi al traffico telefonico fra limiti normativi ed equivoci giurisprudenziali*, in *Cass. pen.*, 1999, 480. Secondo l'Autore, «i dati informativi [...] sono, in fatto, elaborati e memorizzati dal gestore del servizio di telefonia, indipendentemente dalla richiesta di acquisizione dell'autorità giudiziaria». Pertanto, i tabulati– divenuti *ex post* rilevanti a fini investigativi o processuali – possono essere acquisiti soltanto nell'eventualità in cui si dia avvio al procedimento penale.

[871] Le indagini preliminari (artt. 326 c.p.p. e ss.) costituiscono la prima fase del procedimento penale e hanno inizio con la ricezione da parte della polizia giudiziaria o del pubblico ministero della notizia di reato (art. 330 c.p.p.); terminano quando quest'ultimo decide di esercitare l'azione penale o di richiedere al giudice l'archiviazione della notizia di reato (art. 408 c.p.p). Per un approfondimento sul punto, si rinvia a TONINI, *Manuale di procedura penale*, *cit.*, 512 e ss.

[872] L'espressione si rinviene nella *Risoluzione del XVIII Congresso internazionale di diritto penale*, Istanbul, 20-27 settembre 2009, in *Riv. dir. proc*., 2010, 333.

[873] In tal senso v. NEGRI, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico*, *cit.*, 47.

[874] V. RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico*, *cit.*, 183.

[875] I commi sopracitati sono stati introdotti con la legge 48/2008 di ratifica della Convenzione di Budapest e poi rimasti inalterati nella disciplina attualmente vigente. Per un approfondimento sul punto si veda Cap I § 3.4.

[876] Per un approfondimento sulla procedura in esame si rinvia sempre al Cap. I § 3.4.

[877] Il comma 4-*ter* dell'art. 132 Codice *Privacy* annovera espressamente in siffatto catalogo*:* «Il Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonché gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme delle disp. att. c.p.p.». In dottrina, si è rilevato che la portata soggettiva della norma risulta eccessivamente ampia e variegata. Il tasso di indeterminatezza della disposizione in esame è ulteriormente aumentato dal rinvio ad una norma *extra-codicem*. In tal senso, v. LUPÀRIA, *La ratifica della Covenzione* Cybercrime *del consiglio d'Europa*, in *Dir. pen e proc*., 2008, 721. Sull'ordine di conservazione emesso, invece dal Ministro dell'interno v. NOVELLINO, *Il Viminale può chiedere di conservare i dati*, in *Guida dir.*, 2008, 70.

ordinare ai fornitori dei servizi di comunicazione elettronica la conservazione dei dati di traffico telematico[878] per un periodo pari a novanta giorni. L'ordine di conservazione può essere emesso ai fini dello svolgimento delle investigazioni preventive[879] o per finalità di accertamento dei reati qualora sussistano «motivate esigenze» rilevate da autorità nazionali e straniere.

L'impulso all'iniziativa delle forze di polizia nazionali potrebbe essere determinato, dunque, anche da esigenze di giustizia emergenti in ambito internazionale, in forza del meccanismo di mutua assistenza previsto dall'art. 29 della Convenzione di Budapest[880]. Ciò si verifica quando, nell'ambito della raccolta transnazionale delle "prove digitali", i dati telematici conservati in territorio nazionale siano prossimi ad essere cancellati ai sensi dell'art. 132, comma 1, del Codice *Privacy*. Le autorità italiane possono decidere di estendere il periodo di archiviazione dei dati ai sensi dell'art. 132, comma 4-t*er*, preservando la prova informatica[881] in essi contenuta[882].

---

[878] I commi 4-*ter*, 4-*quater* e 4-*quinquies* si riferiscono soltanto ai dati di traffico telematico, escludendo dall'ambito di applicazione della disciplina i tabulati telefonici. La scelta del legislatore di circoscrivere la portata applicativa della norma non deve stupire, in quanto i dati traffico telematico o c.d. "metadati" esclusi i dati traffico telefonico. In tal senso, v. FORLANI, *La conservazione preventiva di dati informatici per l'accertamento dei reati*, in *Dir. internet*, 2008, 520.

[879] Si fa riferimento alle indagini preventive previste dall'art. 226 disp. att. c.p.p. rubricato «Intercettazioni e controlli preventivi sulle comunicazioni». Ai fini del lavoro, è utile riportare integralmente i commi 4 e 5 del suddetto articolo:

«Con le modalità e nei casi di cui ai commi 1 e 3, può essere autorizzato il tracciamento delle comunicazioni telefoniche e telematiche, nonché l'acquisizione dei dati esterni relativi alle comunicazioni telefoniche e telematiche intercorse e l'acquisizione di ogni altra informazione utile in possesso degli operatori di telecomunicazioni (comma 4).

In ogni caso gli elementi acquisiti attraverso le attività preventive non possono essere utilizzati nel procedimento penale, fatti salvi i fini investigativi. In ogni caso le attività di intercettazione preventiva di cui ai commi precedenti, e le notizie acquisite a seguito delle attività medesime, non possono essere menzionate in atti di indagine né costituire oggetto di deposizione né essere altrimenti divulgate (comma 5).

[880] L'art. 29, paragrafo 1, del Convenzione di Budapest dispone che «Una Parte può richiedere ad un'altra Parte di ordinare od ottenere in altro modo la conservazione rapida di dati immagazzinati attraverso un sistema informatico, situato nel territorio di quest'altra Parte e nei confronti della quale la Parte richiedente intende avanzare una richiesta di mutua assistenza per la perquisizione o altro simile mezzo di accesso, per il sequestro o altro strumento simile, o per la divulgazione dei dati».

[881] Per una definizione di "prova informatica" o c.d. "*digital evidence*" si veda, in dottrina, ZICCARDI, *Scienze forensi e tecnologie informatiche*, in LUPÁRIA e ZICCARDI, *Investigazione penale e tecnologia informatica*, Milano, 2007, 4; DANIELE, *Le caratteristiche della prova digitale*, in *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali* a cura di RUGGIERI e PICOTTI, Torino, 2011, 203 e ss.; RICCI, Digital evidence*, sapere tecnico-scientifico e verità giudiziale*, in *Scienza e processo penale* a cura di CONTI, Milano, 2011, 347.

[882] Cfr. ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, *cit.*, 176.

In base a siffatte premesse, emerge che la procedura di congelamento dei dati telematici può essere attivata dalle autorità esecutive già durante le attività di investigazione, e cioè quando sia stato ancora avviato un procedimento penale. Anche in assenza di *notitia crimis*, la polizia giudiziaria, e non solo[883], ha la possibilità di richiedere i dati "esterni" alle comunicazioni elettroniche e tutte le informazioni in essi contenute. Questi potranno essere utilizzati sia durante le investigazioni sia nella fase dell'«accertamento», e cioè nell'eventualità che abbia avuto origine un procedimento penale a carico utente i cui dati sono stati conservati.

Ai sensi dell'art. 132, comma 4-*ter,* tale operazione di natura preventiva è posta in essere «per finalità di accertamento e repressione di specifici reati». Quest'ultima formula non contribuisce a delimitare l'ambito applicativo della norma, che anzi risulta eccessivamente fluida e generica[884]. In assenza di una espressa precisazione dei reati nei confronti dei quali si può procedere – che, invece, vengono definiti soltanto «specifici» – si deduce che gli organi esecutivi possano emettere l'ordine di conservazione dei dati di traffico non soltanto ma per qualsiasi reato, e non soltanto per i fatti di criminalità grave.

Se tramite il richiamo all'art. 226 delle disp. att. c.p.p. il legislatore sembra conferire alla polizia giudiziaria un potere limitato a casi eccezionali e urgenti da esercitarsi entro un lasso di tempo determinato, l'assenza di limiti di natura oggettiva rischia di erodere la componente di eccezionalità[885]. La dicitura ambigua del comma 4-*ter* delinea, dunque, uno strumento esperibile per qualunque tipo di reato e rimesso alla discrezionalità della polizia, anche laddove l'invasività della misura non è giustificata da urgenti esigenze di giustizia.

Grazie al dominio di siffatta mole di elementi di natura eterogenea, l'autorità esecutiva acquisisce un monopolio strategico[886] nel campo della giustizia penale,

---

[883] In particolar modo, si tratta del «Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonché gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale».

[884] Cfr. FORLANI, *La conservazione preventiva di dati informatici per l'accertamento dei reati*, in *Dir. internet*, 2008, 520.

[885] È opportuno rammentare, per completezza di esposizione, che l'art. 226 comma 1 norme att. c.p.p. subordina l'esecuzione delle intercettazioni preventive alla necessità di acquisire «notizie concernenti la prevenzione dei delitti di cui all'art. 407 comma 2, lett. a), n. 4 e 51 comma 3 bis c.p.p.».

[886] In tal senso NEGRI, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico), cit.,* 46.

molto prima dell'intervento del magistrato[887]. Ciò non solo realizza un'alterazione degli equilibri di potere, ma contribuisce ad instaurare un meccanismo di *mass surveillance*[888] per finalità di pubblica sicurezza. In una fase antecedente all'instaurazione del procedimento penale, le autorità esecutive hanno la possibilità di conservare i dati di traffico telematico di qualsiasi utente, indipendentemente dalla sua implicazione in un procedimento penale. Chiunque faccio uso di strumenti di comunicazione elettronica è, dunque, trattato come "sospettato" ancor prima che un fatto di reato venga ad esistenza.

L'individuo non è più presunto innocente, bensì colpevole, fino a prova contraria. Siffatto assunto legittima, anzi rende necessario, agire prima che il fatto di reato sia commesso e intercettare in via preventiva tutti comportamenti che potranno dare adito ad illeciti di natura penale[889].

Al termine di questa breve disamina, è evidente che l'istituto della c.d. *data retention*, così come disciplinato nel Codice *Privacy*, sollevi una serie di dubbi di compatibilità rispetto a principi di diritto processuale penale, riconosciuti in Costituzione. La normativa attuale consente il verificarsi di una serie di momenti che, di fatto, aggirano le modalità acquisitive tassativamente individuate dal legislatore vanificando il diritto a rimanere in silenzio, il diritto a non collaborare con il potere giudiziario e il privilegio contro l'autoincriminazione[890]. Inoltre, l'effettiva potenzialità auto-incriminatrice dei dati "esterni" alla comunicazione realizza una rimarchevole compressione della presunzione di non colpevolezza, soprattutto quando si procede ai sensi dell'art. 132, comma 4-*ter*, del Codice *Privacy*.

---

[887] L'art. 4-*quiquies* prevede che «I provvedimenti adottati ai sensi del comma 4-*ter* sono comunicati per iscritto, senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione il quale, se ne ricorrono i presupposti, li convalida. In caso di mancata convalida, i provvedimenti assunti perdono efficacia».

[888] Il rischio che l'istituto della *data retention* venga a concretizzarsi in fenomeno di *mass surveillance* è stato evidenziato dal Presidente del Garante *Privacy* Antonio Soro durante il convegno "Privacy digitale e protezione dei dati personali tra persona e mercato", svoltosi a Firenze il 24 ottobre 2017. Sul punto si rimanda a quanto detto *supra*.

[889] Inoltre, il fenomeno sopradescritto genera un'incontrollata espansione dei poteri riconosciuti in capo alle autorità inquirenti e la «trasmutazione poliziesca» del procedimento penale. NEGRI, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico), cit.,* 46.

[890] Cfr.PANSINI, *Diritto di difesa*, in AA. VV. *Diritti della persona e nuove sfide del processo penale., cit.*, 278.

CONCLUSIONI

Giunti sin qui, è opportuno ripercorrere il *fil rouge* del presente lavoro, traendo le dovute conclusioni: operazione non certo agevole, posto che l'istituto della *data retention* continua ad essere al centro di un dibattito in perpetua evoluzione che contribuisce a renderlo fascinante oggetto di studio.

Come si è avuto modo di approfondire, la possibilità di comprimere un serie di valori individuali di rango fondamentale per acquisire elementi probatori utili all'accertamento penale implica la necessità di trovare un punto di equilibrio tra esigenze contrapposte, riassumibili con il "binomio sicurezza-tutela dei diritti". Infatti, la formulazione di uno o più capi di imputazione, ancorché provvisori, nei confronti di una determinata persona dà origine ad un rapporto dialettico tra pubblica autorità e individuo[891]. Siffatta tensione, da un lato legittima l'impiego da parte della prima di strumenti di natura coercitiva, di ricerca e di acquisizione probatoria che, per natura, limitano le libertà fondamentali previste in Costituzione; dall'altro, attribuisce al singolo – *rectius*, "all'accusato"[892] – una serie di diritti e prerogative personali da esercitare contro gli organi inquirenti. Pertanto, il soggetto nei confronti del quale viene formulato un addebito penale è titolare sia di diritti di natura processuale[893], che trovano attuazione nel corso dell'accertamento del reato, sia dei diritti fondamentali[894] riconosciuti ad ogni individuo indipendentemente dal suo eventuale coinvolgimento in un procedimento penale. In questo senso, il processo, quale "luogo di esperienza della coercizione statale"[895], diviene teatro in cui si consuma l'antico scontro tra Stato e cittadino, tra "autorità" e "libertà"[896].

---

[891] In questi termini si è espresso FELICIONI, *Accertamenti sulla persona e processo penale. Il prelievo di materiale biologico*, Assago, 2007, 29.

[892] In questo contesto, l'espressione "accusato" non ha un preciso significato giuridico, ma viene utilizzato in senso a-tecnico per ricomprendere sia la figura dell'indagato sia la figura dell'imputato.

[893] Cfr. CASELLA, *Sul valore probatorio del contegno non collaborativo dell'imputato nell'accertamento del fatto proprio*, in *Questione Giustizia*, 2.

[894] Tra i quali rientrano i diritti costituzionali che formano il blocco delle tre inviolabilità (artt. 13, 14 e 15 Cost.). «Rispetto a questi ultimi il processo non è tanto il luogo di radicamento della relativa garanzia, bensì il luogo in cui operano i meccanismi garantistici previsti per la tutela di tali diritti, nell'ipotesi in cui si renda eventualmente necessaria una loro limitazione». GREVI, *Garanzie individuali ed esigenze di difesa sociale nel processo penale*, in *Alla ricerca di un processo penale "giusto". Itinerari e prospettive*, Milano, 2000, 13; UBERTIS, *Sistema di procedura penale*, Torino, 2004, 175.

[895] L'espressione è di NEGRI, *Compressione dei diritti di libertà e principio di proporzionalità*, 2019, 57.

[896] Il processo penale viene, infatti, considerato «Il prototipo della contrapposizione tra autorità e libertà». Siffatto «irriducibile antagonismo connaturato nella sua esistenza» è riflesso nel codice di procedura penale, i cui contenuti sono strettamente rispondenti ai valori della società democratica in cui

Onde evitare che le istanze securitarie e preventive siano perseguite mediante meccanismi surrettizi volti ad alterare il principio di legalità e l'assetto di garanzie costituzionali[897], è opportuno individuare i confini di un'attività investigativa e di indagine, sempre più pervasiva e avvantaggiata dai nuovi strumenti della tecnica. Dinanzi ad un siffatto scenario, questo studio si è posto l'obiettivo di verificare, mediante l'esame trasversale di aspetti sostanziali e procedurali, se l'attività di conservazione dei dati di traffico, così come attualmente regolamentata nell'ordinamento nazionale, realizzi un equilibrio tra le esigenze contrapposte sopradescritte o se invece privilegi uno dei due aspetti a discapito dell'altro.

Nel rispondere al suddetto quesito, si è ritenuto necessario, dapprima, inquadrare i termini in conflitto, oltretutto evocati nel titolo del presente lavoro. Dopo aver specificato a cosa si allude, *in subiecta materia*, quando si parla di "pubblica sicurezza" la cui accezione ampia è tale da ricomprendere l'esigenza collettiva di prevenzione e accertamento dei reati, si è dimostrato in che modo la c.d. *data retention* si riveli uno strumento utile a tale fine. In tal senso, si è riscontrato che i dati "esterni" alla comunicazione, in quanto dotati di una notevole "potenzialità euristica"[898], siano in grado di divulgare diversi aspetti della personalità di un individuo. Infatti, mediante l'accesso ai tabulati telefonici e telematici, gli organi inquirenti hanno la possibilità di ricostruire non solo gli spostamenti del cittadino cui è intestata l'utenza mobile di cui sono acquisiti i dati di traffico ma anche i contatti che quest'ultimo abbia stabilito in un determinato lasso di tempo[899].

In base a siffatte evidenze, si è osservato che l'attività acquisitiva dei dati "esterni" alla comunicazione rappresenti uno strumento indispensabile per le indagini, a cui è impossibile rinunciare *in toto*. Gettando uno sguardo sull'evoluzione normativa in materia di *data retention,* si è visto come tale utilità sia stata progressivamente messa a fuoco dal legislatore nazionale che, superata la difficoltà iniziale nell'inquadramento

---

sono introiettati. Sul punto si veda NEGRI, *Compressione dei diritti di libertà e principio di proporzionalità*, 2019, 58; in termini analoghi KALB, *Introduzione*, in AA. VV. *Diritti della persona e nuove sfide del processo penale. Atti del XXXII convegno nazionale* (Salerno, 25-27 ottobre 2018), Milano, 2019, 19; MAZZA, *L'interrogatorio e l'esame dell'imputato nel suo procedimento*, Milano, 2004, 2.

[897] Cfr. CONTI, *Sicurezza e riservatezza, in Dir. pen e proc,* 2019, 1572.

[898] L'espressione è di ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, *cit.*, 33.

[899] Cfr. Cap. I § 4.1.

dell'istituto, ne ha via via ampliato la portata applicativa mediante la semplificazione delle procedure. Da un complesso sistema normativo rispondente alla logica del "doppio binario"[900] sia nella determinazione dei periodi di conservazione dei dati sia nella bipartizione dell'*iter* acquisitivo[901], si è passati ad un regime semplificato che faciliti l'accesso ai tabulati di traffico da parte degli organi inquirenti. Inoltre, con la novella del 2018[902], si è realizzata una dilatazione dei tempi di archiviazione soltanto apparentemente limitata ai reati gravi e di criminalità organizzata, ma, di fatto, estesa a tutte le fattispecie penali, a riprova di un tendenziale approccio "securitario" del legislatore nostrano.

Spesso intervenuto a seguito di attentati terroristici di matrice internazionale, quest'ultimo ha, infatti, dato prova di privilegiare le esigenze di accertamento e repressione dei reati a discapito delle istanze di segno contrario, volte a salvaguardare i diritti fondamentali coinvolti[903]. Mediante la predisposizione di una disciplina di *data retention* eccessivamente invasiva nella "sfera privata" del singolo, si è osservato come, nell'ordinamento interno, non sia ancora stato raggiunto un equilibrio tra i termini in conflitto di cui *supra*. La normativa relativa all'attività acquisitiva dei dati di traffico nel procedimento penale, così come cristallizzata nel Codice *Privacy*, risulta "sbilanciata" sul fronte avanzato della tutela della sicurezza.

Al fine di impostare correttamente siffatta problematica e di tracciare le coordinate di una possibile soluzione, volta al contemperamento tra esigenze contrapposte, si è ritenuto opportuno approfondire il secondo termine del conflitto evocato nel titolo del presente contributo: i diritti fondamentali della persona. In tal senso, si è proceduto all'individuazione dell'ampio catalogo di situazioni giuridiche soggettive, rinvenibili nella topografia costituzionale nonché nella Carta di Nizza[904], con le quali interferisce la metodologia investigativa in analisi in esame. Tradizionalmente considerata uno strumento di investigazione meno invasivo rispetto ad altri istituti di natura

[900] Riguardo alla logica del doppio binario e alla scelta di graduare la tutela del diritto alla riservatezza in base al tempo in cui si siano svolte le telefonate si è spesso in senso critico CAMON, *L'acquisizione dei dati sul traffico delle comunicazioni, cit.,* 594.
[901] L'evoluzione del quadro normativo in materia di *data retention* è stata ampliamente approfondito nel Cap. I § 3 a cui si rinvia.
[902] Si fa riferimento all'art. 132, comma 5-*bis*, del Codice *Privacy* inserito con il d.lgs. 10 agosto 2018, n. 101.
[903] Cfr. Cap I §3.4 e 3.6.
[904] Il punto è stato oggetto di trattazione nel Cap. II a cui si rinvia.

processuale[905], si è, infatti, dimostrato che la c.d. *data retention*, al pari di altri strumenti frutto della rivoluzione tecnologica[906], sia in grado di interferire con una serie di "valori"[907] ascrivibili al concetto di "riservatezza". Originariamente intesa come libertà "negativa", essa è diventata oggetto, negli ultimi anni, di un sistema di tutela "multivello" (c.d. *multilevel protection*) in cui concorrono più ordinamenti giuridici tra di loro correlati: l'assetto normativo nazionale ed europeo[908].

Ciò posto, tra il novero di beni giuridici aggrediti dall'istituto della c.d. *data retention* sono stati richiamati, dapprima, la libertà di domicilio (art. 14 Cost.) e la segretezza della comunicazione (art. 15 Cost.), intesi alla luce della loro nuova "dimensione tecnologica"[909]. L'attività di acquisizione dei dati di traffico, così come disciplinata nel Codice *Privacy*, sembra, infatti, interferire non solo con il "nucleo essenziale" dei diritti richiamati, ma, soprattutto, con la protezione che essi accordano ad esigenze di tutela emerse di recente. Ad esempio, si è evidenziato come la metodologia investigativa in esame realizzi una compressione della libertà domiciliare mediante il tracciamento degli spostamenti del singolo, ma anche un'interferenza rispetto al "luogo" virtuale all'interno del quale l'individuo esprime la propria personalità, il c.d. "domicilio informatico"[910].

In secondo luogo, lo scenario dei diritti fondamentali coinvolti dalla c.d. *data retention* è stato ampliato tramite il ricorso alla Convenzione europea dei diritti dell'uomo e delle libertà fondamentali e alla Carta dei diritti fondamentali dell'Unione europea. In particolar modo, si è sottolineato come quest'ultima abbia realizzato un ulteriore traguardo evolutivo in materia di *privacy* mediante la configurazione della c.d. *data protection* quale autonomo diritto della persona di rango fondamentale. In ambito comunitario si è, dunque, perfezionata la messa a fuoco di un nuovo paradigma

---

[905] Cfr. sentenza Corte cost., 11 marzo 1993, n. 81, in *www.cortecostituzionale.it.* Cfr. Cap. 1 § 2.
[906] Sul punto v. *Introduzione.*
[907] In tale sede, il termine "valore" è utilizzato nell'accezione intesa da GROSSI, *Prima lezione di diritto*, Roma-Bari, 2003, 20. L'Autore specifica che «Il valore è un principio o comportamento che la coscienza collettiva ritiene di sottolineare isolandolo e selezionandolo dal fascio indistinto dei tanti princìpi e comportamenti; isolandolo e selezionandolo lo sottrae alla relatività che è propria del fascio indistinto, gli conferisce senza dubbio una qualche assolutezza, lo costituisce come modello».
[908] Sul punto, v. ANDOLINA, *L'ammissibilità degli strumenti di captazione dei dati personali tra standard di tutela della* privacy *e onde eversive*, cit., 918.
[909] Cfr. Cap III.
[910] *Ab origine*, il concetto di c.d. domicilio informatico è stato elaborato nell'ordinamento nazionale in riferimento ai reati informati e, nella specie, al reato di accesso abusivo a un sistema informatico o telematico ai sensi dell'art. 615-*ter* c.p. L'argomento è stato approfondito nel Cap. II § 3.1 a cui si rinvia.

normativo attinente alla «dimensione esterna» della riservatezza[911], con cui l'istituto *de quo* entra in contrasto.

Pertanto, non è un caso che sia stata proprio la Corte di Giustizia Ue a superare per la prima volta la tesi circa la modesta "invasività" dell'attività acquisitiva dei tabulati di traffico telefonico e telematico, tradizionalmente sostenuta dalla giurisprudenza italiana. Come si è avuto modo di approfondire, i giudici di Lussemburgo hanno, dunque, riconosciuto l'elevata "potenzialità euristica" dei dati di traffico, che, sebbene esulino dal contenuto della comunicazione, consentono di trarre precise conclusioni riguardo alle abitudini giornaliere degli individui, ai luoghi di residenza permanente o temporanea, ai loro spostamenti e le loro attività nonché sulle relazioni sociali da essi stabilite. In una straordinaria veste di "giudice costituzionale"[912], la Corte di Lussemburgo ha affermato, inoltre, che l'attività di accesso e di estrazione dei dati da parte delle pubbliche autorità costituisca di per sé un'ingerenza dei diritti fondamentali tutelati dagli articoli 7 e 8 della Carta di Nizza, da considerarsi particolarmente grave in quanto priva del consenso dell'interessato.

Dalle considerazioni che precedono, è emerso un dato inconfutabile: l'istituto della *data retention*, sebbene di indubbia utilità per l'accertamento penale, risulta idoneo ad interferire sia con le tradizionali "libertà negative" (artt. 14[913] e 15[914] Cost.) sia con la tutela della "sfera privata" del singolo (7 CDFUE)[915] e con il diritto di ciascuno a mantenere il controllo sui propri dati personali (8 CDFUE)[916]. Pertanto, per evitare di dover rinunciare *in toto* a tale metodologia di indagine correndo il rischio di arrecare un danno eccessivo alle esigenze di pubblica sicurezza, è necessario che questa sia oggetto di una regolamentazione in piena conformità alla cornice di valori costituzionali coinvolti. Rievocando i termini utilizzati all'inizio di tale disamina, è opportuno, dunque, che si realizzi un contemperamento tra le istanze riassunte mediante il binomio "sicurezza-tutela dei diritti".

---

[911] Cfr. LUPÁRIA, Privacy*, diritti della persona e processo penale,* in *Rivista di diritto processuale*, LXXIV (6), 2019, 1452.
[912] L'espressione è di TRUCCO, *Data retention: la Corte di Giustizia si appella alla Carta UE dei diritti fondamentali*, in *Giur. it*., 2014, 1580.
[913] Sul punto si veda Cap II § 3.
[914] Cfr. Cap. II § 2.
[915] Cfr. Cap II § 6.
[916] Per l'esegesi dell'art. 8 della Carta di Nizza si rimanda II § 7.

Le direttrici mediante le quali è possibile attuare tale bilanciamento in materia di *data retention*, sono state individuate ancora una volta dalla Corte di Giustizia Ue. A partire dalla storica sentenza *Digital Ireland e Seitlinger*[917] fino alla recentissima pronuncia *H.K. Danmark*[918], si è visto come i giudici di Lussemburgo abbiano indicato il principio di proporzionalità come "criterio moderatore" in base al quale verificare la legittimità dell'interferenza realizzata dallo Stato nella "sfera privata" del singolo ogniqualvolta si predisponga l'acquisizione dei dati di traffico. In conformità di siffatto canone, le autorità inquirenti che procedono all'accesso dei tabulati di traffico e telematico sono tenute a sottoporre la richiesta al vaglio di un giudice o di un'autorità amministrativa indipendente, a verificarne la ragionevolezza rispetto alle esigenze del caso concreto secondo i parametri della idoneità e della "stretta necessità", e a darne conto mediante atto motivato[919]. Soltanto mediante l'adozione di tali *standard* di natura processuale e sostanziale, secondo la Corte di Giustizia Ue, è possibile evitare ingiustificate compressioni dei diritti fondamentali convolti dalla *data retention* e, allo stesso tempo, assecondare le esigenze di repressione e accertamento dei reati.

Dalle considerazioni *de qua,* è scaturito un processo di revisione critica[920] avente ad oggetto non solo la disciplina comunitaria, tramite l'invalidazione della direttiva 2006/24/CE in materia di conservazione dei dati di traffico, ma anche gli assetti normativi nazionali. Da qui, l'esigenza di affrontare, nel presente lavoro, la questione circa la compatibilità della disciplina italiana relativa all'attività di acquisizione dei dati rispetto agli arresti giurisprudenziali europei. Ciò non solo alla luce del principio del primato dell'ordinamento sovranazionale rispetto a quello interno, ma soprattutto per verificare se la normativa cristallizzata nell'art. 132 del Codice *Privacy* raggiunga il tanto "agognato" equilibrio tra interessi contrapposti, o se invece propenda, come si è anticipato, per le esigenze di pubblica sicurezza.

A tal fine, si è proceduto all'analisi di tutte le interferenze esistenti tra la disciplina italiana relativa all'attività acquisitiva dei dati di traffico e gli *standard* di tutela in

[917] Si fa riferimento alla Corte giust. UE, Gr. Sez., sent. 8 aprile 2014, *Digital Rights Ireland*, oggetto di ampia disamina nel Cap. § 9.
[918] Cfr. Corte giust. UE, Gr. Sez., sent. 2 marzo 2021, *H.K. Danmark,* approfondita nel Cap II § 11.
[919] Sul punto v. ANDOLINA, *L'ammissibilità degli strumenti di captazione dei dati personali tra standard di tutela della* privacy *e onde eversive*, in *Arch. pen.*, 2015, n. 3, 936.
[920] Cfr. ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, Milano, 2018, 3.

punto di proporzionalità, determinatezza e di stretta necessità, individuati dalla Corte Giustizia Ue. Al termine di siffatta disamina, si è avuto modo di constatare che l'art. 132 del Codice *Privacy* risulti incompatibile rispetto al diritto comunitario sotto una serie di profili. In tale sede, è opportuno ricordare a titolo meramente esemplificativo: la previsione di obbligo di conservazione "generalizzata" in capo ai *service providers*, l'assenza di intervento dell'autorità giurisdizionale durante la fase acquisitiva dei tabulati e l'eccessiva dilatazione del periodo di archiviazione dei dati[921]. Tutti elementi che depongono a favore del fatto circa l'idoneità della normativa italiana a soddisfare i requisiti procedurali e sostanziali rilevati in ambito comunitario.

Nonostante ciò, la giurisprudenza italiana si è rivelata piuttosto "ostile" nel riconoscere siffatta evidenza, riservando un atteggiamento coerente con l'approccio securitario dapprima riscontrato nei confronti del legislatore nazionale. Gettando uno sguardo sugli approdi interpretativi dei giudici nazionali[922] – sia di merito sia di legittimità – si è avuto modo di costatare una certa "resistenza" dinanzi alle novità provenienti dall'Unione europea, volte a garantire la tutela prioritaria dei diritti di rango fondamentale coinvolti dalla *data retention*. Si è così osservato come i giudici italiani abbiano non solo perseverato nel fornire una interpretazione "restrittiva" ai principi emanati in ambito sovranazionale ma, soprattutto, abbiano sempre negato l'incompatibilità dell'art. 132 Codice *Privacy* rispetto all'assetto normativo europeo. Soltanto di recente, sono stati emessi dei provvedimenti di segno contrario relativi all'acquisizione dei dati di traffico che fanno ben sperare nel tanto atteso *revirement* da parte dei giudici italiani[923]. Per la prima volta, sembra riconoscersi da parte della giurisprudenza nazionale il contrasto tra gli *standard* europei e la normativa italiana, su più fronti inidonea ad assicurare il corretto bilanciamento tra esigenze di accertamento dei reati e di tutela dei diritti fondamentali.

Dinanzi a siffatto approdo ermeneutico innovativo, si ritiene quanto mai auspicale l'intervento novellatore del legislatore italiano che, lungo le coordinate segnate dal principio di proporzionalità, modifichi la disciplina in materia di *data retention* per renderla coerente con l'assetto normativo interno e sovranazionale. Soprattutto a fronte delle sopradescritte istanze di provenienza comunitaria, è indubbia la criticità della

[921]Cfr. Cap. III § 3.
[922] Cfr. III § 4.2.
[923] Cfr. Cap III § 4.3.

disciplina relativa all'attività di conservazione dei dati di traffico che, privilegiando esigenze di pubblica sicurezza, realizzi un sacrificio eccessivamente ampio della "sfera privata" dell'individuo, contravvenendo ai profili essenziali che regolano il rito penale. Infine, mediante siffatto intervento del legislatore, potrà essere finalmente concessa la meritata stabilità alla disciplina della *data retention,* costantemente soggetta ad oscillazioni tra istanze contrapposte.

BIBLIOGRAFIA

ADDIS, *Diritto all'autodeterminazione informativa e processo penale in Germania, in AA. VV., Protezione dei dati personali e accertamento penale*, (a cura di) NEGRI, Roma, 2007, 97.

AMATO, *Individuo e autorità nella disciplina della libertà personale,* Milano, 1976.

ID., *Il reato grave facilita l'accesso al tabulato*, in *Guida dir*., 2004, 31.

ANDOLINA, *L'ammissibilità degli strumenti di captazione dei dati personali tra standard di tutela della* privacy *e onde eversive*, in *Arch. pen.*, 2015, n. 3, 916.

ID., *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, Milano, 2018.

APRILE-SPEZIA, *Le intercettazioni telefoniche ed ambientali. Innovazioni tecnologiche e nuove questioni giuridiche*, Milano, 2004.

ARENA, *La Corte di Giustizia sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento*, in *Quad. Cost*., 2014, 722.

ATERNO, *Commento all'art. 10*, in AA. VV., *L'attuazione della Convenzione di europea sul cybercrime. Commento alla legge 18 marzo 2008 n. 48*, Milano, 2008, 70.

ATERNO, CISTERNA, *Il legislatore interviene ancora sulla* data retention*, ma non è finita*., in *Dir. Pen. e proc*., 2009, 279.

ID., *Conservazione dei dati informatici e prospettive europee. Relazione svolta al Convegno dell'OLAF (Milano, 23-25 gennaio 2008),* Milano*,* 2009, 163.

ID., *Le investigazioni informatiche e l'acquisizione della prova digitale*, in *Giur. merito,* 2013, 955.

BACCARI, *Il trattamento (anche elettronico) dei dati personali per finalità di accertamento dei reati*, in AA. VV., *Cybercrime,* (a cura di) CADOPPI, CANESTRARI, MANNA, PAPA, Torino, 2019, 1599.

BALDASSARRE, *Diritti inviolabili*, in *Diritti della persona e valori costituzionali*, Torino, 1997, 61.

BALDUCCI, *Le garanzie nelle intercettazioni tra costituente e legge ordinaria*, Milano, 2002.

BALSAMO-TAMIETTI, *Le intercettazioni tra garanzie formali e sostanziali*, in AA.VV., *Giurisprudenza europea e processo penale italiano*, BALSAMO E KOSTORIS (a cura di), Torino, 2008, 463.

BARILE, CHELI, *Corrispondenza (libertà di)*, in *Enc. Dir*., vol. X, Milano, 1962, 744.

BARBERA, *Commento all'art. 2 della Costituzione*, in *Commentario della Costituzione*, BRANCA (a cura di), Bologna, 1997.

BARLETTA, *Il* "legal privilege" *come principio fondamentale ed i suoi limiti: il caso della normativa antiriciclaggio*, su *www.forumcostituzionale.it*.

BARTOLI, *Lotta al terrorismo internazionale. Tra diritto penale del nemico*, jus in bello *del criminale e annientamento del nemico assoluto*, Torino, 2008.

BENE, *Il pedinamento elettronico: truismi e problemi spinosi*, in AA.VV., *Le indagini atipiche,* SCALFATI (a cura di), Torino, 2014, 347.

BELLANTONI, *Sequestro probatorio e processo penale*, Piacenza, 2005.

ID., *Art. 248*, in *Codice di procedura penale commentato*, GIARDA, SPANGHER (a cura di), Milano, 2017, 2440.

BELLAVISTA, TRANCHINA, *Lezioni di diritto processuale penale*, Milano, 1987

BERRUTI, *Un* vulnus *al diritto alla* privacy *per la lotta contro il terrorismo*, 2016, in *www.legislazionepenale.eu.*

BIN, PITRUZZELLA, *Diritto costituzionale,* Torino, 2020.

BOLOGNINI, PELINO, BISTOLFI, *Il regolamento* Privacy *europeo: commentario alla nuova disciplina sulla protezione dei dati personali,* Milano, 2016.

BONETTI, *Riservatezza e processo penale*, Milano, 2003.

BRAGHÒ, *Le indagini informatiche tra esigenze di accertamento e garanzie di difesa*, in *Dir. inf. e informatica*, 2005, 524.

ID., *L'ispezione e la perquisizione di dati, informazioni e programmi informatici,* in LUPARIA (a cura di), *Sistema penale e criminalità informatica*, Milano, 2009,193.

BRICOLA, *Prospettive e limiti della tutela penale della riservatezza*, in *Riv. It. Dir. proc. Pen*., 1967, 1088.

BRIGHI, *Cibercrimine e anonimato in Rete. Riflessioni su sicurezza, efficacia investigativa e tutela delle libertà personali*, in *Sicurezza e scienze sociali*, 2017, n. 3, 29.

BRUNO, *Intercettazioni di comunicazioni o conversazioni*, in *Digesto delle discipline penalistiche*, Torino, 1993, 178.

BUSETTO, *La Commissione Europea torna ad occuparsi del mercato unico digitale: una prima analisi della proposta del nuovo regolamento in tema di comunicazioni elettroniche*, in *www.filodiritto.it.*

BUSIA, *Si volta pagina sulla tenuta dei tabulati telefonici*, in *Guida dir.*, 2003, 40.

ID., *Elenco tassativo delle informazioni da archiviare*, in *Guida dir*., 2004, 29.

ID., *Così la riservatezza "guadagna" terreno*, in *Guida dir*., 2004, 58.

ID., Privacy *a rischio per la durata della conservazione,* in *Guida dir.,* 2009, 77.

CAGGIANO, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione,* in *Medialaws – Rivista dir. media*, 2018, 64.

CALAMANDREI, *Acquisizione dei dati esteriori di una comunicazione ed utilizzazione delle prove cd. costituzionali*, in *Giur. It*., 1999, 1691.

CAIANELLO, *Il principio di proporzionalità nel processo penale, in Dir. pen. contemp.*, 2014, 143.

ID., *Dal terzo pilastro ai nuovi strumenti: diritti fondamentali, "road map" e l'impatto delle nuove direttive*, in *Dir. pen. cont.*, 2015, 78.

ID., *You can't always counterbalance what you want,* in *European Journal of Crime, Criminal Law and Criminal Justice*, 2017, 283.

CAJANI, *Alla ricerca del* log *(perduto),* in *Dir. Internet*, 2006, 572.

ID., *Investigazioni vs.* privacy: *il bilanciamento di opposti interessi.* in AA.VV. Computer forensics *e indagini digitali. Manuale tecnico giuridico e casi pratici,* Vol. I, Forlì, 2011, 333.

CAJANI, ATERNO, *La disciplina in tema di conservazione dei dati* (data retention), in AA.VV. Computer forensics *e indagini digitali. Manuale tecnico giuridico e casi pratici*, Forlì, 2011, 249.

CAMON, *Le intercettazioni nel processo penale*, Milano, 1996.

ID., *L'acquisizione dei dati sul traffico delle comunicazioni,* in *Riv. it. dir. e proc. pen*., 2005, 594.

ID., *Cavalli di Troia in Cassazione*, in *Archivio della nuova procedura penale*, 2017, 95.

ID., *La fase che "non conta e non passa": indagini governate dalla legge?,* in *Dir. Pen. e processo*, 2017, 425.

CAPOROTUNDO, *Presunzioni legali e onere della prova nel processo penale*, 2017, in *www.giurisprudenzapenale.it.*

CAPUTO, *La conservazione dei dati di traffico telefonico e telematico nella normativa antiterrorismo*, in *Archivio penale*, 2016, 28.

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

CARETTI, BARBIERI, *I diritti fondamentali: Libertà e diritti sociali*, Torino, 2017, 345.

CARNEVALE, *Autodeterminazione informativa e processo penale: le coordinate costituzionali,* in NEGRI, *Protezione dei dati e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?, Roma,* 2007, 3.

CARTABIA, *Le sentenze «gemelle»: diritti fondamentali, fonti, giudici*, in *Giur. cost.*, 2007, 3564.

CARUSO*, La libertà e la segretezza delle comunicazioni nell'ordinamento nazionale, in Forum di Quaderni Costituzionali, Rassegna,* 2013, n. 10, 2.

CASCIONE*, I diritti fondamentali prevalgono sull'interesse alla sicurezza: la decisione* data retention *della Corte di Giustizia e gli echi del* datagate, in *Nuova Giur. Comm*., 2014, 11039.

CASELLA, *Sul valore probatorio del contegno non collaborativo dell'imputato nell'accertamento del fatto proprio*, in *Questione Giustizia*, 1.

CASTELLS, *The information age: economy, Society and Culture*. *Volume 1: The Rise of the Network Society*, Oxford, 2010.

CAVALLARI, *La capacità dell'imputato*, Milano, 1968.

CAVALIERE, *Questioni attuali in tema di "nuovi diritti"*, in *www.dirittifondamentali*, 2015, 12.

CLEMENTI, *La Costituzione italiana: commento articolo per articolo*, Bologna, 2018, 53.

CISTERNA, *Il legislatore interviene ancora sulla data retention, ma non è ancora finita*, in *Dir. pen e proc*. 2009, 279.

ID., *Cedu e diritto alla* privacy, in GAITO (a cura di), *I principi europei del processo penale*, Roma, 2016, 194.

ID., Data retention: *termine di sei anni per la custodia dei dati*, in *Guida al Diritto,* 2018, 97.

COLOMBO, *La sentenza del caso di Garlasco e la computer forensics: analisi di un complesso rapporto tra diritto e informatica*, in *Cyberspazio e diritto*, 2010, 277.

ID., "Data retention" *e Corte di giustizia: riflessioni a prima lettura sulla declaratoria di invalidità della direttiva: riflessioni a prima lettura sulla declaratoria di invalidità della direttiva 2006/24/CE*, in *Cass. pen*., 2014, 2705.

COMOGLIO, *Art. 24, 3° co.*, in *Comm. Cost.,* BRANCA (a cura di), Bologna-Roma, 1981, 1.

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

ID., *L'attuazione della direttiva Frattini: un bilanciamento insoddisfacente tra riservatezza e diritto alla prova*, in AA. VV., *Le nuove forme sulla sicurezza pubblica*, LORUSSO (a cura di), Padova, 2008, 3.

ID., *L'acquisizione dei tabulati (cd.* data retention*)*, in TONINI, CONTI, *Il diritto delle prove penali*, Milano, 2014, 470.

ID., *Sicurezza e riservatezza, in Dir. pen e proc.,* 2019, 1572.

CORDERO, *Procedura penale*, Milano, 2003, 285.

CORTESE, *La protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona*, in *Il dir. dell'Ue*, 2013, 315.

COSTANZO, *Il ruolo del fattore tecnologico e le trasformazioni del costituzionalismo*, in *Associazione Italiana dei Costituzionalisti, Costituzionalismo e globalizzazione. Atti del XXVII Convegno Annuale.* (Salerno 22-24 novembre 2012), Napoli, 2014, 43.

CUOMO, *La prova digitale*, in CANZIO-LUPÀRIA (a cura di), *Prova scientifica e processo penale*, Milano, 2018, 724.

D'AGOSTINO, *La tutela penale dei dati personali nel riformato quadro normativo: un primo commento al D.Lgs. 10 agosto 2018, n. 101, in Archivio penale*, 2019, 1.

DANIELE, *Le caratteristiche della prova digitale*, in *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali,* RUGGIERI e PICOTTI (a cura di), Torino, 2011, 203.

ID., *La prova digitale nel processo penale*, in *Riv. dir. proc.,* 2011, 283.

ID., La vocazione espansiva delle indagini informatiche e l'obsolescenza della legge, in *Proc. Pen. e giustizia*, 2018, 831.

DANIELE, AMADEO, *Diritto dell'Unione europea: sistema istituzionale, ordinamento, tutela giurisdizionale, competenze*, Milano, 2020, 326.

D'AMICO, *Commento all'art. 27*, in BIFULCO, CELOTTO, OLIVETTI (a cura di), *Commentario alla Costituzione della Repubblica italiana*, Torino 2006, 556.

DI FILIPPI, *Dati esteriori delle comunicazioni e garanzie costituzionali*, in *Giur. It.*, 1995, 117.

DINACCI, *Localizzazione attraverso celle telefoniche*, in AA. VV., *Le indagini atipiche,* SCALFATI (a cura di), Torino, 2014, 369.

DI PAOLO, *Tecnologie del controllo e prova penale: l'esperienza statunitense e spunti per la comparazione*, Padova 2008.

ID., *La prova informatica*, in *Enc. Dir.*, 2013, 737.

DE LEO, *La conservazione dei dati di traffico telefonico e telematico nella prospettiva europea*, in *Dir. pen. proc.*, 2002, 1016.

DI MARTINO, *Le intercettazioni telematiche e l'ordinamento italiano: una convivenza difficile*, in *Ind. pen*., 2002, 223.

ID*., Il* Bundesverfassungsgericht *dichiara l'incostituzionalità della* data retention *e torna sul rapporto tra libertà e sicurezza*, in *Giur. Cost.,* 2010, 4059.

DOMINIONI, *Imputato*, in *Enc. Dir.,* XX, Milano, 1970, 794.

DONINI, *Europeismo giudiziario e scienza penale. Dalla dogmatica classica alla giurisprudenza-fonte*, Milano, 2011.

EASTON, *Silence and Confessions. The Suspect as the Source of Evidence*, New York, 2014.

ELIA, *Le misure di prevenzione tra l'art. 13 e l'art. 25 della Costituzione,* in *Giur. cost.,* 1964, 951.

GREVI, «Nemo tenetur se detegere». *Interrogatorio dell'imputato e diritto al silenzio nel processo penale italiano*, Milano, 1972.

FABBRINI, *Lotta al terrorismo e tutela dei dati personali alla luce della sentenza Irlanda c. Parlamento e Consiglio*, in *Quaderni Costituzionali*, 2009, 419.

ID., *The European Court of Justice Ruling in the Data Rentention Case and its Lessons for Privacy and Surveillance in the U.S.*, in *Harvard Human Rights Journal,* 2015, 65.

FATTA, *La tutela della* privacy *alla prova dell'obbligo di data retention e delle misure antiterrorismo*, in *Dir. dell'informatica e dell'informazione*, 2008, 395.

FELICIONI, *Accertamenti sulla persona e processo penale. Il prelievo di materiale biologico*, Assago, 2007.

FERRAJOLI, *Diritto e ragione. Teoria del garantismo penale*, Bari-Roma, 1996.

FERRUA, *Difesa (Diritto di)*, in *Dig. Pen*., 3, Torino, 1998, 466.

ID., *Il "giusto processo" in Costituzione*, in *Dir. giust.*, 2000, 78.

FILIPPI*, L'intercettazione di comunicazioni*, Milano, 1997.

ID., *Il rilevamento del «tracciato axe»: una nuova denominazione per una vecchia tecnica di indagine, in Giur. Ita.,* 1999, 1687.

ID., *Una disciplina per i tabulati telefonici che attua il diritto alla prova: un modello anche per le intercettazioni?* in *Studi urbinati di scienze giuridiche, politiche ed economiche.* Nuova serie A, vol. 58, 2007, 438.

ID., *Intercettazioni, tabulati e altre limitazioni della segretezza delle comunicazioni*, in *Procedura penale. Teoria e pratica del processo*, SPANGHER, MARANDOLA, GARUTI e KALB (diretto da), Torino, 2015, 1132.

ID., *La disciplina italiana dei tabulati telefonici e telematici contrasta con il diritto u.e.*, 2021, in *www.dirittodifesa.ue.*

FINOCCHIARO, *La giurisprudenza della Corte di giustizia in materia di dati personali da "Google Spain" a "schrems", in Dir. inf.,* 2015, 779.

FLOR, *Investigazioni ad alto contenuto tecnologico e tutela dei diritti. Fondamentali della persona nella recente giurisprudenza del Bundesverfassungsgericht: la decisione del 27 febbraio 2008 sulla Online Durchsung e la sua portata alla luce della sentenza del 2.3.2010 sul data retention,* in *Ciberspazio e dir.*, 2010, 359.

ID., *Data retention e limiti al potere coercitivo dello stato in materia penale: le sentenze del* Bundesverfassungsgericht *e della* Curtea Constitutionala, in *Cass. pen*., 2011, 1952.

ID., *La Corte di giustizia considera la direttiva europea 2006/24 sulla cd*. "data retention" *contraria ai diritti fondamentali. Una lunga storia a lieto fine?* in *Dir. Pen. contemp.,* 2014,178.

ID., *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 "jure condendo"*, in RESTA – ZENO-ZENOVICH, *Il diritto all'oblio su Internet dopo la sentenza* Google Spain, Roma, 2015, 223.

ID., *Data retention ed art. 132 cod. privacy: vexata quaestio (?)*, in *Dir. Pen. Contemp*., 29 marzo 2017.

FRATTALLONE, *Il trattamento nel processo penale*, in PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, Milano, 2006, 1364.

FRIGO, *Così le scelte sulla valutazione delle prove vanificano le conquiste sul giusto processo*, in *Guida Dir*., 1999, 48.

ID., *Nella conservazione dei dati internet la necessaria tutela giurisdizionale*, in *Guida dir.*, 2004, n. 18, 14.

GAITO, FURFARO, *Intercettazioni: esigenze di accertamento e garanzie della riservatezza*, in GAITO (a cura di), *I principi europei del processo penale*, Roma, 2016, 363.

GALETTA, *Il principio di proporzionalità fra. Diritto nazionale e diritto europeo (con uno sguardo anche al di là dei confini dell'Unione Europea)*, in *Riv. It. Dir. pubbl. comun*., 2019, 927.

GIARDA, SPANGHER, GARUTI, BERNASCONI, *Codice di procedura penale commentato*, Assago, 2017.

GIORDANO, *Tabulati telefonici: senza regole sull'*iter *"convivenza" più difficile con la novella*, in *Guida dir.*, 2004, 12.

GREVI, *Garanzie individuali ed esigenze di difesa sociale nel processo penale*, in *Alla ricerca di un processo penale "giusto". Itinerari e prospettive*, Milano, 2000.

GROPPI, *sub* art. 7*,* in *L'Europa dei diritti, commento alla Carta dei diritti fondamentali dell'Unione Europea*, in BIFULCO, CARTABIA, CELOTTO (a cura di), Bologna, 2001, 351.

GROSSI, *Prima lezione di diritto*, Roma-Bari, 2003.

GUARNIERI, *Lineamenti di diritto comparato*, Milano, 2020.

GUELLA, *Data retention e circolazione dei livelli di tutela dei diritti in Europa: dai giudizi di costituzionalità rivolti alla disciplina UE al giudizio della Corte di giustizia rivolto alle discipline nazionali*, in *DPCE on line*, n. 2, 2017, 349.

KALB, *Introduzione*, in AA. VV. *Diritti della persona e nuove sfide del processo penale. Atti del XXXII convegno nazionale* (Salerno, 25-27 ottobre 2018), Milano, 2019, 19.

KOSTORIS, *La lotta al terrorismo e alla criminalità organizzata tra speciali misure processuali e tutela dei diritti fondamentali nella risoluzione del XVIII Congresso internazionale del diritto penale*, in *Riv. dir. proc*., 2010, 330.

ID., *Il nuovo pacchetto antiterrorismo, tra prevenzione, contrasto in rete e centralizzazione delle indagini*, KOSTORIS, VIGANO', Il nuovo pacchetto antiterrorismo, Giappichelli, Torino, 2015, XV.

KOSTORIS, BALSAMO, *Manuale di procedura penale europea*, Milano, 2019,

LAMBERIGTS, *The Privilege Against Self- Incrimination*, *In New Journal of European Criminal Law,* 2016, 42.

LARONGA, *Le prove atipiche nel processo penale*, Padova, 2002, 55.

ID., Le attività urgenti di investigazione informatica e telematica, in LUPÀRIA (a cura di), Sistema penale e criminalità informatica, Milano, 2009, 152.

LORENZETTO, *Utilizzabilità dei dati informatici incorporati su* computer *in sequestro: dal contenitore al contenuto passando per la copia*, in *Cass. pen.*, 2010, 532.

LORUSSO, "Digital evidence", "cybercrime" *e giustizia penale 2.0*, in *Processo penale e Giustizia*, 2019, 821.

LUPÀRIA, ZICCARDI, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, 2007.

ID., *La ratifica della Covenzione* Cybercrime *del consiglio d'Europa*, in *Dir. pen e proc*., 2008, 72.

ID., *Internet Provider* e giustizia penale: modelli di responsabilità e forme di collaborazione processuale, Milano, 2012.

ID., MARAFIOTI, *Confessione, liturgie della verità e macchine sanzionatorie. Scritti raccolti in occasione del Seminario di studio sulle «Lezioni di Lovanio» di Michel Foucault*, Torino, 2015.

ID., Data retention *e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, in *Giur. Pen*., 2019, 758.

ID., *Privacy, diritti della persona e processo penale,* in *Rivista di diritto processuale*, LXXIV (6), 2019, 1448.

ID., *Diritto alla* privacy, in AA. VV. *Diritti della persona e nuove sfide del processo penale. Atti del XXXII convegno nazionale* (Salerno, 25-27 ottobre 2018), Milano, 2019, 98.

ILLUMINATI, *La presunzione di innocenza dell'imputato,* Bologna, 1979.

ID., *La disciplina processuale delle intercettazioni*, Milano, 1983.

ID., Libertà e segretezza della comunicazione, in AA. VV. *Diritti della persona e nuove sfide del processo penale. Atti del XXXII convegno nazionale* (Salerno, 25-27 ottobre 2018), Milano, 2019, 157.

IOVENE, Data retention *tra passato e futuro. Ma quale presente?* in *Cass. Pen*., 2014, 4274.

ITALIA, *Libertà e segretezza della corrispondenza e delle comunicazioni,* Milano, 1963.

MANTOVANI, *Diritto alla riservatezza e libera manifestazione del pensiero con riguardo alla pubblicità dei fatti criminosi*, in *Arch. Giur*., 1968, 61.

MARAFIOTI, *Scelte autodifensive dell'indagato e alternative al silenzio*, Torino, 2000.

ID., Digital evidence *e processo penale,* in *Cass. pen*., 2011, 4510.

MARCHETTI, *Testis contra se. L'imputato come fonte di prova nel processo penale dell'età moderna*, Milano, 1994.

MARCOCCIO, Data retention, *cosa prevede la direttiva europea,* 2007, in *www.interlex.it*

ID., Data retention*, la "Pisanu" dovrà fare i conti con l'Europa*, 2007, in *www.interlex.it*.

MARCOLINI., *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen*., 2015, 779.

ID., *Prove atipiche (diritto processuale penale)*, in Enc. Dir.-Annali, vol. X, Milano 2017, 695.

ID., *L'istituto della* data retention *dopo la sentenza della corte di giustizia del 2014* in AA. VV., *Cybercrime,* (a cura di) CADOPPI, CANESTRARI, MANNA, PAPA, Torino, 2019, 1579.

MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Torino, 2007.

ID., *Tabulati telefonici*, in *Enc. Dir.-Annali*, vol. III, Milano, 2010, 1111.

MARINUCCI, DOLCINI, GATTA, *Manuale di diritto penale. Parte generale*, Milano, 2018.

MARTINICO, *Commento all'art. 7 della Carta*, in MASTROIANNI, POLLICINO, ALLEGREZZA, PAPPALARDO, RAZZOLINI, *Carta dei diritti fondamentali dell'Unione europea*, Milano 2017, 116.

MARSHALL, THOMAS, *Privacy and Criminal Justice*, Basingstoke, 2017.

MAZZA, *L'interrogatorio e l'esame dell'imputato nel suo procedimento*, Milano, 2004.

MELILLO, *Intercettazione ed acquisizione dei tabulati telefonici: un opportuno intervento correttivo delle Sezioni Unite,* in *Cass. pen*, 1999, 473.

MILIZIA, *Stop all'onere generalizzato di conservazione dei dati trasmessi con ogni mezzo di comunicazione*, in *Dir. e giust*., 2016, n. 105, 9.

MONTAGNA, *Libertà domiciliare*, in AA. VV. *Diritti della persona e nuove sfide del processo penale. Atti del XXXII convegno nazionale* (Salerno, 25-27 ottobre 2018), Milano, 2019, 119.

NEGRI, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico),* in *Archivio penale*, 2016, n. 1, 44.

ID., *Compressione dei diritti di libertà e principio di proporzionalità*, in AA. VV. *Diritti della persona e nuove sfide del processo penale. Atti del XXXII convegno nazionale* (Salerno, 25-27 ottobre 2018), Milano, 2019, 55.

NINO, *L'annullamento del regime della conservazione dei dati di traffico nell'Unione europea da parte della Corte di giustizia UE: prospettive ed evoluzioni future del sistema europeo di* data retention, in *Diritto dell'Unione Europea,* 2014, 803.

NOVELLINO, *Il Viminale può chiedere di conservare i dati*, in *Guida dir.*, 2008, 70.

OLIVETTI, *Brevi note in materia di libertà di comunicazione*, in *Giur. Cost*., 1996, 3858.

ORLANDI, *Inchieste preparatorie nei procedimenti di criminalità organizzata: una riedizione dell'*inquisitio generalis?, in *Riv. it. dir. proc. pen.*, 1996, 568.

ID., *Il processo nell'era* di internet, in *Dir. pen. proc*., 1998, 140.
OROFINO, *La libertà di espressione tra Costituzione e Carte europee dei diritti. Il dinamismo dei diritti in una società in continua formazione*, Torino, 2014.

ID., *Garanzie individuali ed esigenze repressive (ragionando intorno al diritto di difesa nei procedimenti di criminalità organizzata)*, in AA.VV. *Studi in ricordo di G. Pisapia. Procedura penale II*, Milano, 2000, 560.

ID., *Relazione introduttiva*, in *Delitto politico e diritto penale del nemico*, GAMBERINI, ORLANDI (a cura di), Bologna, 2007, 35.

ID., *La riforma del processo penale fra correzioni strutturali e tutela progressiva dei diritti fondamentali*, in *Rivista italiana di diritto e procedura penale*, 2014, 1136.

PACE, *Art. 15 Cost*., in BRANCA (a cura di), *Commentario della costituzione, Art. 13-20 – Rapporti Civili*, Bologna-Roma, 1977.

ID., *Nuove frontiere della libertà di "comunicare riservatamente" (o, piuttosto, del diritto alla riservatezza)?*, in *Gir. Cost.*, 1993, 742.

ID., *Problematica delle libertà costituzionali. Parte generale*, Padova, 2003.

PAEFFGEN, *"Verpolizeilichung" des Strafprozesses – Chimäre oder Gefahr?* in *Zur Theorie und Systematik des Strafprozeßrechts*, Berlino, 1995, 16.

PANSINI, *Diritto di difesa*, in AA. VV. *Diritti della persona e nuove sfide del processo penale. Atti del XXXII convegno nazionale* (Salerno, 25-27 ottobre 2018), Milano, 2019, 277.

PARODI, *Le intercettazioni*, Torino, 2002.

ID., *Le modifiche del "d.l. giustizia" in tema di conservazione dei dati*, in *Dir. pen. Proc.*, 2004, 544.

PASCALI, *La* data retention *dopo la dichiarazione di invalidità della Direttiva 2006/24/CE*, in *Riv. elettronica dir. econ. Manegement*, 2015, 3, 87.

PATRONO, Privacy *e vita privata*, in Enc. dir., vol. XXXV, Milano, 1986, 574.

PAULESU, *Presunzione di non colpevolezza,* in *Digesto pen.,* Torino, 1995, 674.

PELINO, ALAGNA, BOLOGNINI, *Codice della disciplina privacy*, Milano, 2019.

PELOSO, *L'approvazione della direttiva 2016/2019 sul patrocinio a spese dello Stato: la battuta finale nel cammino verso la mappatura dei diritti procedurali fondamentali*, *in www.legislazionepenale.eu.*

PISANI, *La tutela penale della "riservatezza": aspetti processuali*, in *Riv. it. dir. proc. pen*., 1967, 785.

PIZZETTI, *La privacy come diritto fondamentale alla protezione dei dati personali nel Trattato di Lisbona*, in BILANCIA, D'AMICO, *La nuova Europa dopo il Trattato di Lisbona*, Milano, 2011, 85.

ID., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, 153.

PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislative e beni giuridici tutelati*, in AA. VV., *Il diritto penale dell'informatica nell'epoca di internet*, PICOTTI (a cura di), Padova, 2004, 21.

ID., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Legge 18 marzo 2008, n. 48., in Diritto penale e processo,* 2008, n. 6, 696.

ID., *Diritto penale e tecnologie informatiche: una visione di insieme,* in AA. VV., *Cybercrime,* CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), Torino, 2019, 33.

PISANI, *La tutela penale della riservatezza: aspetti processuali*, in *Riv. It. Dir. proc. Pen.*, 1967, 786.

POTETTI, *Corte costituzionale n. 81/93: la forza espansiva della tutela accordata dall'art. 15 comma 1 Cost.*, in *Cass. Pen*., 1993, 2746.

POLICE, *Commento all'art. 24*, in BIFULCO, CELOTTO, OLIVETTI (a cura di), *Commentario alla Costituzione della Repubblica italiana*, Torino, 2006, 502.

POLLICINO, *Diritto all'oblio e conservazione dei dati. La Corte di giustizia a piedi uniti: verso un* digital right to privacy, in *Giur. Cost*., 2014, 2949.

ID., *Commento all'art. 8 della Carta*, in MASTROIANNI, POLLICINO, ALLEGREZZA, PAPPALARDO, RAZZOLINI, *Carta dei diritti fondamentali dell'Unione europea*, Milano, 2017, 141.

POLLICINO, BASSINI, *La Corte di Giustizia una trama ormai nota: la sentenza* Tele2 Sverige *sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, in *Dir. Pen. Cont.*, 2017, 1.

POTETTI, *Corte Costituzionale n.81/1993: la forza espansiva della tutela accordata dall'art. 15 comma 1 della Costituzione*, in *Cass. Pen.*, 1993, 2746.

PULITANÒ, *La posta in gioco nella decisione della Corte costituzionale sulla sentenza Taricco*, in *Dir. pen. cont*., 2016, 1, 236.

PUSTORINO, *Corte costituzionale, Cedu e controlimiti (Nota a Corte cost., 28 novembre 2012, n. 264, Inps c. Lorenzon)*, in *Giur. it.*, 2013, 770.

RAFARACI, *Intercettazioni e acquisizioni di tabulati telefonici*, in KOSTORIS, ORLANDI (a cura di), *Contrasto al terrorismo interno e internazionale,* Torino, 2006, 276.

RENZETTI, *Acquisizione dei dati segnalati sul* display *del cellulare: il rischio di una violazione dell'art. 15 Cost.*, in *Cass. Pen.,* 2006, 542.

RODOTÀ, *La* privacy *tra individuo e collettività,* in *Pol. dir.,* 1974, n. 3, 551.

RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico. - Il bilanciamento tra privacy e repressione del fenomeno criminale nel dialogo tra giurisprudenza e legislatore*, in *Dir. Pen. contemp*., 2016, 156.

RICCI, Digital evidence*, sapere tecnico-scientifico e verità giudiziale*, in *Scienza e processo penale,* CONTI (a cura di), Milano, 2011, 347.

RINALDINI, 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*, 2021, in *www.giurisprudenzapenale.it.*

ROSSI, *Gli accordi PNR ("Passenger Name Record") nella lotta al terrorismo internazionale. Conseguenze del parere n. 1/15 della Corte di giustizia del 26 luglio 2017 per la legittimità della Direttiva n. 2016/681/Ue*, in *Dir. comun. e degli scambi int.*, 2018, 395.

ROXIN, *Involuntary self-incrimination and the right to privacy in Criminal proceedings*, in *Israel Law Review,* 1997, 74.

RUGGIERI, *Divieti probatori e inutilizzabilità nella disciplina delle intercettazioni telefoniche*, Milano, 2001.

ID., Data retention *e giudice di merito penale. Una discutibile pronuncia*, in *Cass. pen*., 2017, 2483.

ID., *Corte europea dei diritti dell'uomo e giudici nazionali, alla luce della più recente giurisprudenza costituzionale (tendenze e prospettive)* in *Osservatorio costituzionale,* 2018, 20.

RUSSO, SCIUTO, *Habeas data e informatica*, Milano, 2011.

SALERNO, *La protezione della riservatezza e l'inviolabilità della corrispondenza,* in NANIA (a cura di), *I diritti costituzionali,* Torino, 2001, 417.

SARTOR, *L'informatica giuridica e le tecnologie dell'informazione – Corso di informatica giuridica*, Torino, 2016.

SCACCIANOCE, *Approvvigionamento di flussi e dati tramite il dispositivo telefonico altrui,* in AA. VV., *Le indagini atipiche,* SCALFATI (a cura di), Torino, 2014, 29.

SCARCELLA, *Presupposti e motivazione del sequestro probatorio*, in *Il libro dell'anno del diritto 2019*, Roma, 2019, 548.

SCELLA, *Per una storia costituzionale del diritto di difesa: la Corte e l'ambiguità del processo "misto"*, In *Il diritto processuale penale nella giurisprudenza costituzionale*, Napoli, 2006, 197.

SCIARABBA, *Le "spiegazioni" della Carta dei diritti fondamentali dell'Unione*, DPCE, 2005, 59.

SEMINARA, *Sorveglianza segreta e nuove tecnologie nel diritto europeo dei diritti umani,* in *Medialaws – Rivista dir. media*, 2017, 133.

SIGNORATO, *Contrasto al terrorismo e* data retention: *molte ombre e poche luci*, in KOSTORIS-VIGANO' (a cura di), *Il nuovo pacchetto antiterrorismo*, Torino, 2015, 83.

ID., *Le indagini digitali – Profili strutturali di una metamorfosi investigativa*, Torino, 2018.

ID., *Novità in tema di* data retention*. La riformulazione dell'art. 132 codice privacy da parte del D. Lgs. 10 agosto 2018 n. 101*, in *Dir. Pen. contemp.*, 2018, 153.

SILVESTRI, *L'individuazione dei diritti della persona*, in *Dir. pen. Cont.*, 2018, 1.

ID., *L'individuazione dei diritti della persona*, in AA. VV. *Diritti della persona e nuove sfide del processo penale. Atti del XXXII convegno nazionale* (Salerno, 25-27 ottobre 2018), Milano, 2019, 21.

STRACUZZI, Data retention: *il faticoso percorso dell'art. 132 Codice* privacy *nella disciplina della conservazione dei dati digitali*, in *Dir. inf.*, 2008, 585.

STROZZI, MASTROIANNI, *Diritto dell'Unione europea. Parte istituzionale*, Torino, 2020.

TESTA, Cybercrime*, intercettazioni telematiche e cooperazione giudiziaria in materia di attacchi ai sistemi informatici*, in *Persona e danno*, *www.personaedanno.it*.

TESAURO, *La ragionevolezza nella giurisprudenza comunitaria*, Napoli, 2012, 43.

TIBERI, *Riservatezza e protezione dei dati personali*, in CARTABIA (a cura di), *I diritti in azione*, Bologna, 2007, 361.

ID.*, La Corte di giustizia sulla conservazione dei dati: la protezione dei diritti fondamentali nel «dopo-Lisbona»,* in *Quad. Cost*., 2014, 722.

TONINI, *Prova scientifica e contraddittorio*, in *Dir. pen. proc*., 2003, 1459.

ID., *Manuale di procedura penale*, Milano, 2019.

TROGU, *Sorveglianza e "perquisizioni"* on-line *su materiale informatico*, in AA.VV., *Le indagini atipiche*, a cura di SCALFATI (a cura di), Torino, 2014, 441.

TRUCCO, Data retention: la Corte di Giustizia si appella alla Carta UE dei diritti fondamentali, in *Giur. it*., 2014, 1580.

UBERTIS, *Sistema di procedura penale*, Torino, 2004, 175.

ID., *I diritti fondamentali nel processo penale, in Sistema di procedura penale. Principi generali*, vol. I, Milano, 2017, 240.

VENEGONI-GIORDANO, *La Corte Costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici,* in *www.dirittopenalecontemporaneo.it*.

VIGANÒ, *Terrorismo, guerra e sistema penale*, in *Riv. it. dir. proc. pen*., 2006, 695.

ID., *Il caso Taricco davanti alla Corte costituzionale: qualche riflessione sul merito delle questioni, e sulla reale posta in gioco*, in *www.penalecontemporaneo.it.*

VIGLIAR, *Privacy e comunicazioni elettroniche: la direttiva 2002/58/CE*, in *Dir. inf.*, 2003, 402.

ID., Data breach *e sicurezza informatica*, in *La Nuova Disciplina Europea della Privacy*, SICA, D'ANTONIO, RICCIO (a cura di), Milano, 2016, 245.

VOENA, *Difesa penale*, in *Enc. Giur. Treccani*, vol. X, Roma, 1988.

WARREN, BRANDEIS, *The Right to Privacy, in Harvard Law Review*, Vol IV, Boston, n. 5, 1890, 193.

WOODS, *Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber),* in *www.eulawanalysis.blogspot.com*.

ZANGHÌ, *La Corte costituzionale risolve un primo contrasto con la Corte europea dei diritti dell'uomo ed interpreta l'art. 117 della Costituzione: le sentenze n. 348 e 349 del 2007*, in *www.giurcost.org*.

ZENO-ZENCOVICH, *Intorno alla decisione nel caso "Schrems": la sovranità digitale e il governo internazionale delle reti di telecomunicazione,* in *Il Diritto dell'informazione e dell'informatica,* 2015, 683.

ZICCARDI, *Scienze forensi e tecnologie informatiche*, in *Investigazione penale e tecnologia informatica*, LUPÁRIA, ZICCARDI, Milano, 2007, 4.

GIURISPRUDENZA

BUNDESVERFASSUNGSGERICHT, sentenza 2 marzo 2010, sez III (1BvR 256/08).

CORTE COSTITUZIONALE ITALIANA sentenza 26 gennaio 1957, n. 4.

CORTE COSTITUZIONALE ITALIANA, sentenza 26 gennaio 1957, n. 30.

CORTE COSTITUZIONALE ITALIANA, sentenza 18 marzo 1957, n. 57.

CORTE COSTITUZIONALE ITALIANA, sentenza 22 dicembre 1961, n. 70.

CORTE COSTITUZIONALE ITALIANA, sentenza 9 giugno 1961, n. 30.

CORTE COSTITUZIONALE ITALIANA, sentenza 13 luglio 1963, n. 133.

CORTE COSTITUZIONALE ITALIANA, sentenza 23 marzo 1966, n. 26.

CORTE COSTITUZIONALE ITALIANA, sentenza 22 marzo 1971, n. 55.

CORTE COSTITUZIONALE ITALIANA, sentenza 6 aprile 1973, n. 34.

CORTE COSTITUZIONALE ITALIANA, sentenza 10 febbraio 1972, n. 27.

CORTE COSTITUZIONALE ITALIANA, sentenza 9 gennaio 1974, n. 2.

CORTE COSTITUZIONALE ITALIANA, sentenza 8 giugno 1984, n. 170.

CORTE COSTITUZIONALE ITALIANA, sentenza 11 luglio 1991, n. 366.

CORTE COSTITUZIONALE ITALIANA, sentenza 11 marzo 1993, n. 81.

CORTE COSTITUZIONALE ITALIANA, sentenza 31 maggio 1996, n. 175.

CORTE COSTITUZIONALE ITALIANA, sentenza 17 luglio 1998, n. 281.

CORTE COSTITUZIONALE ITALIANA, ordinanza 3 aprile 2000, n. 95.

CORTE COSTITUZIONALE ITALIANA, sentenza 14 novembre 2006, n. 32.

CORTE COSTITUZIONALE ITALIANA, sentenza 22 ottobre 2007, n. 348.

CORTE COSTITUZIONALE ITALIANA, sentenza 22 ottobre 2007, n. 349.

CORTE COSTITUZIONALE ITALIANA, sentenza 16 maggio 2008, n. 149.

CORTE COSTITUZIONALE ITALIANA, sentenza 26 giugno 2009, n. 184.

CORTE COSTITUZIONALE ITALIANA, sentenza 28 maggio 2010, n. 188.

CORTE COSTITUZIONALE ITALIANA, sentenza 23 gennaio 2019, n. 38.

CURTEA CONSTITUTIONALA, (Romania), sentenza 8 ottobre 2009.

CORTE DI CASSAZIONE ITALIANA, Cass. Civ., Sez. III, sent. 27 maggio 1975, n. 2129.

CORTE DI CASSAZIONE ITALIANA, Cass. Pen., Sez. Un., sent. 23 febbraio 2000, 2144.

CORTE DI CASSAZIONE ITALIANA, Cass. Pen., Sez. VI, sent. 11 febbraio 2002, n. 9331.

CORTE DI CASSAZIONE ITALIANA, Cass. pen, Sez. Un., sent. 28 maggio 2003, n. 36747.

CORTE DI CASSAZIONE ITALIANA, Cass. Pen., Sez. IV, sent. 24 febbraio 2005, n. 20558.

CORTE DI CASSAZIONE ITALIANA, Cass., Pen., Sez. II, sent. 25 ottobre 2005, 41936.

CORTE DI CASSAZIONE ITALIANA, Cass. Pen., Sez. IV, sent. 23 giugno 2009, n. 38160.

CORTE DI CASSAZIONE ITALIANA, Cass., Pen. Sez. V, sent. 10 Marzo 2010, n. 19491.

CORTE DI CASSAZIONE ITALIANA, Cass. Pen., Sez. VI, sent. 14 gennaio 2011, n. 8353.

CORTE DI CASSAZIONE ITALIANA, Cass. Pen., Sez. V, sent. 16 marzo 2012, n. 22577.

CORTE DI CASSAZIONE ITALIANA, Cass. Civ., Sez. I, 28 gennaio 2016, n. 1625.

CORTE DI CASSAZIONE ITALIANA, Cass. Pen., Sez. IV, sent. 19 luglio 2017, n. 50998.

CORTE DI CASSAZIONE ITALIANA, Cass. Pen., Sez. V, sent. 24 aprile 2018, n. 33851.

CORTE DI CASSAZIONE ITALIANA, Cass. Pen., Sez. V, sent. 22 gennaio 2019, n. 2932.

CORTE DI CASSAZIONE ITALIANA, Cass. Pen., Sez. III, 25 settembre 2019, n. 48737.

CORTE DI CASSAZIONE ITALIANA, Cass. Pen., Sez. III, sent. 23 agosto 2019, n. 36380.

CORTE DI CASSAZIONE ITALIANA, Cass. Pen., Sez. II, sent., 10 dicembre 2019, n. 5741.

CORTE DI CASSAZIONE ITALIANA, Cass. Pen., Sez. II, sent. 11 dicembre 2020, n. 35447.

CORTE EUROPEA DEI DIRITTI DELL'UOMO, *Klass e altri c. Germania*, n. 5029/71, sent. 6 settembre 1978.

CORTE EUROPEA DEI DIRITTI DELL'UOMO, *Malone c. Regno Unito*, n. 8691/79, sent. 2 agosto 1984.

CORTE EUROPEA DEI DIRITTI DELL'UOMO, *Funke c. Francia*, n. 10828/84, sent. 25 febbraio 1993.

CORTE EUROPEA DEI DIRITTI DELL'UOMO, *John Murray c. Regno Unito*, n. 18731/91, sent. 8 febbraio 1996.

CORTE EUROPEA DEI DIRITTI DELL'UOMO, *Foucher c. Francia*, n. 22209/93, sent. 18 marzo 1997.

CORTE EUROPEA DEI DIRITTI DELL'UOMO, *Rotaru c. Romania*, n. 28341/95, sent. 4 maggio 2000.

CORTE EUROPEA DEI DIRITTI DELL'UOMO, *Allan c. Regno Unito*, n. 48539/99, sent. 5 novembre 2002.

CORTE EUROPEA DEI DIRITTI DELL'UOMO, *O'Halloran e Francis c. Regno Unito,* nn. 15809/02 e 25624/02, sent. 25 ottobre 2005.

CORTE EUROPEA DEI DIRITTI DELL'UOMO, *Bobek c. Polonia*, n. 68761/01, sent. 17 luglio 2007.

CORTE EUROPEA DEI DIRITTI DELL'UOMO, *S. e Marper c. Regno Unito*, nn. 30562/04 e 30566/04, sent. 4 dicembre 2008.

CORTE EUROPEA DEI DIRITTI DELL'UOMO, *Uzun c. Germania*, n. 35626/05, sent. 2 settembre 2010.

CORTE EUROPEA DEI DIRITTI DELL'UOMO, *Szabó e Vissy c. Ungheria*, n. 37138/14, sent. 12 gennaio 2016.

CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, Grande Sezione, sent., 1° dicembre 1965, *Schwarze c. Einfuhr und Vorratsstelle für Getreide und Futtermittel*, causa C- 16/95.

CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, Grande Sezione, sent. 16 gennaio 1974, *Rheinmühlen Düsseldorf c. Einfuhr und Vorratsstelle für Getreide und Futtermittel*, causa C-166/73.

CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, Grande Sezione, sent. 29 gennaio 2008, *Promusicae c. Telefonica de Espana Sau,* causa C-275/06.

CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, Grande Sezione, sent. 10 febbraio 2009, *Irlanda c. Parlamento europeo*, causa C-301/06.

CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, Grande Sezione, sent. 9 marzo 2010, *Raffinerie Mediterranee (ERG) SpA e altri c. Ministero dello Sviluppo economico e altri*, causa C-378/08.

CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, Grande Sezione, sent. 9 novembre 2010, *Volker* und *Markus Schecke GbR* e *Hartut Eifert* c. *Land Hessen*, cause riunite C-92/09 e C-93/09.

CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, Grande Sezione, sent. 1° marzo 2011, *Association Belge des Consommateurs Test-Achats ASBL* e altri c. *Conseil des ministres*, causa C-236/09.

CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, Grande Sezione, sent. 8 aprile 2014, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e altri e Kärntner Landesregierung e altri*, cause riunite C-293/12 e C-594/12.

CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, Grande Sezione, sent. 13 maggio 2014, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos, Mario Costeja González,* causa C-131/12.

CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, Grande Sezione, sent. 11 settembre 2014, A c. B e altri, causa C-112/13.

CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, Grande Sezione, sent. 8 settembre 2015, *Taricco e altri*, causa C-105/14.

CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, Grande Sezione, sent. 6 ottobre 2015, *Maximillian Schrems c. Data Protection Commissioner*, causa C- 362/14.

CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, Grande Sezione, sent. 5 aprile 2016, *Puligienica Facility Esco (PFE) c. Airgest SpA*, causa C- 2011/04.

CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, Grande Sezione, sent. 21 dicembre 2016, *Tele2 Sverige Ab c. Post-och telestyrelsen, e Secretary of State for the Home Department c. Watson e altri*, cause riunite C-203/15 e C-698/15.

CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, Grande Sezione, sent. 2 ottobre 2018, *Ministerio Fiscal*, causa C-207/16.

CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, Grande Sezione, sent. 6 ottobre 2020, *La Quadrature du Net e altri c. Premier ministre, Garde des Sceaux, ministre de la Justice e altri,* cause riunite C-511/18, C-512/18 e C-520/18.

CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, Grande Sezione, sent. 6 ottobre 2020, *Privacy International c. Secretary of State for Foreign and Commonwealth Affairs e altri*, causa C-623/17.

CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA, Grande Sezione, sent. 2 marzo 2021, *H.K. c. Prokuratuur*, causa C-746/18.

CORTE SUPREMA AMMINISTRATIVA BULGARA, sez. III, sentenza 11 dicembre 2008, n. 13627,

TRIBUNALE ORDINARIO DI PADOVA, Sezione Penale, ordinanza del 15 marzo 2017.

TRIBUNALE ORDINARIO DI ROMA, Sezione Penale, decreto g.i.p del 25 aprile 2021.

TRIBUNALE ORDINARIO DI ROMA, Sezione Penale, decreto g.i.p del 29 aprile 2021.

TRIBUNALE ORDINARIO DI RIETI, Sezione Penale, ordinanza del 4 maggio 2021.