GIUSTIZIA INSIEME

Diritto UE

Dalla conservazione generalizzata a quella mirata e rapida

La Corte di giustizia ridelinea i contorni della *data retention*

di Federica Resta

7 aprile 2022

ABSTRACT

Sviluppando, in maniera più articolata, principi già affermati in passato, la Corte di giustizia chiarisce come la conservazione dei tabulati a fini di accertamento e perseguimento dei reati non possa essere generalizzata e indifferenziata ma soltanto "mirata" sulla base di criteri soggettivi, geografici o di altra natura (purché oggettivi e non discriminatori) ovvero "rapida" (quick freeze). I principi affermati dalla Corte suggeriscono l'opportunità di una riflessione sulla compatibilità, con la disciplina europea, di quella interna, già peraltro recentemente riformata a seguito della sentenza del 2 marzo 2021.

Sommario: 1. **Il contesto** – 2. **Le indicazioni della Corte** – 3. **I riflessi sulla disciplina interna**

1. Il contesto

Con la sentenza del 5 aprile, la Corte di giustizia fornisce alcune, ulteriori indicazioni importanti sulla disciplina della *data retention*, suscettibili d'incidere profondamente sulla stessa natura di questo strumento investigativo.

A distanza di poco più di un anno dalla sentenza H.K. c. Prokuratuur (C 746-18)– con cui si è sottolineata l'esigenza di terzietà, rispetto al soggetto pubblico richiedente, dell'autorità titolare del potere di acquisizione dei tabulati **[1]**- la Corte torna su di un aspetto centrale della disciplina: i presupposti per la legittima conservazione dei dati di traffico a fini "di giustizia".

Sviluppando ulteriormente e chiarendo i principi già affermati con le sentenze rese nel caso Tele2 Sverige (cause riunite C 203/15 e C 698/15) il 21 dicembre 2016 e La Quadrature du Net (C 511/18 e a.) del 6 ottobre 2020, la Corte di giustizia afferma oggi che:

> l'articolo 15, paragrafo 1, della direttiva 2002/58/CE come modificata dalla direttiva 2009/136/CE non consente, a fini di contrasto della "*criminalità grave e di prevenzione delle minacce gravi alla sicurezza pubblica*" la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione, ma ammette:
>
> - la conservazione mirata dei dati relativi al traffico e dei dati relativi all'ubicazione che sia delimitata, sulla base di elementi oggettivi e non discriminatori, in funzione delle categorie di persone interessate o mediante un criterio geografico, per un periodo temporalmente limitato allo stretto necessario, ma rinnovabile;
> - la conservazione generalizzata e indifferenziata degli indirizzi IP attribuiti all'origine di una connessione, per un periodo temporalmente limitato allo stretto necessario;
> - la conservazione generalizzata e indifferenziata dei dati relativi all'identità civile degli utenti di mezzi di comunicazione elettronica, e
> - il ricorso a un'ingiunzione rivolta ai fornitori di servizi di comunicazione elettronica, mediante una decisione dell'autorità competente soggetta a un controllo giurisdizionale effettivo, di procedere, per un periodo determinato, alla conservazione rapida dei dati relativi al traffico e dei dati relativi all'ubicazione di cui dispongono tali fornitori di servizi;
>
> sempre che tali misure garantiscano, "*mediante norme chiare e precise, che la conservazione dei dati di cui trattasi sia subordinata al rispetto delle relative condizioni sostanziali e procedurali e che le persone interessate dispongano di garanzie effettive contro il rischio di*

abusi";

l'articolo 15, paragrafo 1, della citata direttiva 2002/58 è incompatibile con una "*normativa nazionale in forza della quale il trattamento centralizzato delle domande di accesso a dati conservati dai fornitori di servizi di comunicazione elettronica, provenienti dalla polizia nell'ambito della ricerca e del perseguimento di reati gravi, è affidato a un funzionario di polizia, assistito da un'unità istituita all'interno della polizia che gode di una certa autonomia nell'esercizio della sua missione e le cui decisioni possono essere successivamente sottoposte a controllo giurisdizionale*";

il diritto dell'Unione non consente la limitazione temporale, da parte del giudice, degli effetti di una declaratoria di invalidità di una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione, in quanto incompatibile con l'articolo 15, paragrafo 1, della citata direttiva 2002/58, pur essendo l'ammissibilità degli elementi di prova così ottenuti soggetta al principio di autonomia procedurale degli Stati membri, sempreché nel rispetto, in particolare, dei principi di equivalenza e di effettività.

Sotto il primo profilo, la Corte riprende e valorizza quanto affermato nella sentenza Tele2 Sverige, che ha dichiarato incompatibile con la direttiva 2002/58 (letta retroattivamente alla luce della Carta di Nizza e riespansa a seguito dell'invalidazione della 2006/24 ad opera della sentenza Digital Rights dell'8 aprile 2014) ogni previsione interna che, per fini di contrasto dei reati: a) imponga la conservazione, generale e indiscriminata, di tutti i dati di traffico e relativi all'ubicazione degli utenti dei mezzi; b) legittimi l'accesso delle autorità nazionali competenti ai dati conservati per finalità ulteriori rispetto a quelle di contrasto dei "*serious crimes*", in assenza di un previo vaglio giurisdizionale o comunque di un'autorità amministrativa indipendente e di garanzie relative alla conservazione dei dati nella Ue.

Le discipline interne sulla *data retention* devono pertanto prevedere- osservava la Corte nel 2016- **l**'accessibilità dei dati conservati solo da parte dell'autorità giudiziaria o di un'autorità amministrativa indipendente, in base a circostanze e procedure disciplinate dalla legge per esigenze di accertamento di gravi reati, notificando la misura all'interessato (come già affermato dalla Corte EDU nella sentenza Zakharov del 4.12.15), non appena le esigenze investigative lo consentano.

Ma l'aspetto maggiormente innovativo della pronuncia concerneva l'esigenza di rendere selettiva e mirata la stessa conservazione dei tabulati, limitandola in ragione del tipo di dato, del mezzo di comunicazione considerato, della durata della ritenzione, delle persone coinvolte (che devono avere un collegamento almeno indiretto con la commissione di gravi reati), finanche di criteri geografici che limitino la conservazione ad aree caratterizzate da rischi specifici. Già nel 2016, dunque, la Corte indicava specifici presupposti di ammissibilità della conservazione dei

tabulati, che finivano con il mutarne profondamente la natura stessa di misura preventiva e come tale applicabile massivamente, in vista di un'acquisizione, soltanto eventuale, successiva e retrospettiva, in sede giudiziaria.

In tal modo, la Corte evidenziava un'ulteriore, rilevante implicazione del principio di proporzionalità tra limitazioni dei diritti fondamentali ed esigenze di pubblica sicurezza che- come chiarito nella sentenza Digital Rights del 2014- esige una differenziazione della conservazione dei dati specificamente modulata in base al tipo di delitto, alle esigenze investigative, al tipo di dato e di mezzo di comunicazione utilizzato.

2. Le indicazioni della Corte

Con la sentenza in commento la Corte sviluppa, con maggiore nettezza, quei precedenti, sulla base della considerazione dell'ingerenza della conservazione generalizzata dei tabulati sulla privacy "*della quasi totalità della popolazione senza distinzione, limitazione o eccezione [...], senza che tali persone si trovino, neanche indirettamente, in una situazione idonea a dar luogo ad azioni penali*", tale da dover rappresentare "*l'eccezione e non la regola* " (punti 66 e 65).

La Corte, quindi:

a) conferma la posizione tenuta ne La Quadrature du Net rispetto alla legittimità, ai soli fini di salvaguardia della sicurezza nazionale, del "ricorso a un'ingiunzione che imponga ai fornitori di servizi di comunicazione elettronica di *procedere a una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione, in situazioni nelle quali lo Stato membro interessato affronti una minaccia grave per la sicurezza nazionale che risulti reale e attuale o prevedibile, ove il provvedimento che prevede tale ingiunzione possa essere oggetto di un controllo effettivo, da parte di un giudice o di un organo amministrativo indipendente, la cui decisione sia dotata di effetto vincolante, diretto ad accertare l'esistenza di una di tali situazioni nonché il rispetto delle condizioni e delle garanzie che devono essere previste, e detta ingiunzione possa essere emessa solo per un periodo temporalmente limitato allo stretto necessario, ma sia rinnovabile in caso di persistenza di tale minaccia*". Ad avviso della Corte, infatti, "*l'importanza dell'obiettivo della salvaguardia della sicurezza nazionale, letto alla luce dell'articolo 4, paragrafo 2, TUE, secondo il quale la salvaguardia della sicurezza nazionale rimane di competenza esclusiva di ciascuno Stato membro, supera quella degli altri obiettivi di cui all'articolo 15, paragrafo 1, della direttiva 2002/58, in particolare degli obiettivi di lotta alla criminalità in generale, anche grave, e di*

salvaguardia della sicurezza pubblica. Fatto salvo il rispetto degli altri requisiti previsti all'articolo 52, paragrafo 1, della Carta, l'obiettivo di salvaguardia della sicurezza nazionale è quindi idoneo a giustificare misure che comportino ingerenze nei diritti fondamentali più gravi di quelle che potrebbero giustificare tali altri obiettivi".

La distinzione tra sicurezza nazionale e contrasto della criminalità, anche grave è così delineata dalla Corte: "*l'obiettivo di preservare la sicurezza nazionale corrisponde all'interesse primario di tutelare le funzioni essenziali dello Stato e gli interessi fondamentali della società mediante la prevenzione e la repressione delle attività tali da destabilizzare gravemente le strutture costituzionali, politiche, economiche o sociali fondamentali di un paese, e in particolare da minacciare direttamente la società, la popolazione o lo Stato in quanto tale, quali in particolare le attività di terrorismo* [...]; *a differenza della criminalità, anche particolarmente grave, una minaccia per la sicurezza nazionale deve essere reale ed attuale o, quanto meno, prevedibile, il che presuppone il verificarsi di circostanze sufficientemente concrete, da poter giustificare una misura di conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione, per un periodo limitato. Una minaccia del genere si distingue quindi, per sua natura, per gravità e specificità delle circostanze che la costituiscono, dal rischio generale e permanente rappresentato dal verificarsi di tensioni o di perturbazioni, anche gravi, della pubblica sicurezza o da quello di reati gravi".* La Corte precisa inoltre, in replica a un'eccezione del governo danese, che l'eccezionale conservazione, generalizzata e indifferenziata, dei tabulati a fini di sicurezza nazionale, non legittima comunque, in ogni caso, l'accesso agli stessi nell'ambito di indagini penali.

b) escludendo l'equiparabilità (invocata dalla Commissione), alle esigenze di sicurezza nazionale, del contrasto della criminalità particolarmente grave, esclude che in tale ultimo ambito possa ammettersi la conservazione generalizzata e indifferenziata dei dati di traffico e relativi all'ubicazione, ammettendola soltanto relativamente ai dati relativi all'identità civile degli utenti dei mezzi di comunicazione elettronica e agli indirizzi IP attribuiti alla fonte di una connessione, sempre comunque nel rispetto dei requisiti sostanziali e procedurali già affermati e per un periodo temporalmente limitato allo stretto necessario**[2]** (punti 63, 65, 70). Per tali esigenze, la conservazione dei dati di traffico e relativi all'ubicazione (pur congiunta, se del caso, a quella relativa all'indirizzo Ip e all'identità degli utenti) è ammissibile solo se "mirata" (ovvero delimitata, sulla base di elementi oggettivi e non discriminatori, in funzione delle categorie di persone interessate o mediante un criterio geografico, per un periodo temporalmente limitato allo stretto necessario, ma rinnovabile) o rapida (realizzata cioè mediante provvedimento dell'autorità competente soggetto a un controllo giurisdizionale effettivo, che ingiunga ai

fornitori di procedere, per un periodo determinato, alla conservazione rapida dei dati relativi al traffico e dei dati relativi all'ubicazione di cui dispongono: punto 67).

Con riguardo a tali due ultime ipotesi, la Corte precisa che la conservazione "mirata" deve rispondere a requisiti di ordine soggettivo, spaziale, ovvero su altri presupposti purché obiettivi e non discriminatori, stabiliti dagli Stati "*per garantire che la portata di una conservazione mirata sia limitata allo stretto necessario e per stabilire un nesso, almeno indiretto, tra gli atti di criminalità grave e le persone i cui dati sono conservati*" (punto 83).

Per quanto concerne i requisiti di ordine soggettivo, la conservazione deve riferirsi a persone, l'acquisizione dei cui tabulati possa rivelare una connessione, almeno indiretta, con reati gravi o possa prevenire un grave rischio per la sicurezza pubblica o nazionale (ad es. con riguardo alle persone "*precedentemente identificate, nell'ambito delle procedure nazionali applicabili e sulla base di elementi oggettivi e non discriminatori, come soggetti che costituiscono una minaccia per la sicurezza pubblica o la sicurezza nazionale*" o che, nell'ambito di tale identificazione, fondata su elementi oggettivi e non discriminatori, sono sottoposte "*ad indagine o ad altre misure di sorveglianza in corso o sono iscritte nel casellario giudiziario nazionale ove è menzionata una condanna precedente per atti di criminalità grave che possono comportare un elevato rischio di recidiva*" (punti 77-78).

Il criterio spaziale di delimitazione della conservazione (da individuarsi comunque sulla base di parametri oggettivi e non discriminatori) deve riferirsi alla sussistenza, in una o più zone geografiche "*di una situazione caratterizzata da un rischio elevato di preparazione o di commissione di atti di criminalità grave. Tali zone possono essere, in particolare, luoghi caratterizzati da un numero elevato di atti di criminalità grave, luoghi particolarmente esposti alla commissione di atti di criminalità grave, quali luoghi o infrastrutture frequentati regolarmente da un numero molto elevato di persone, o ancora luoghi strategici, quali aeroporti, stazioni o aree di pedaggi*o" (punto 79). I parametri da considerarsi a tal fine, ovvero l'elevato tasso di criminalità o l'esposizione del luogo al rischio di commissione di gravi reati vengono espressamente ritenuti, dalla Corte, non discriminatori anche in assenza di indizi concreti relativi alla preparazione o alla commissione di specifici atti criminosi nel momento e nella zona considerati (punto 80). Naturalmente, le zone geografiche selezionate possono e, se del caso, devono essere modificate in funzione dell'evoluzione delle condizioni che ne hanno giustificato l'individuazione, adeguando dunque la misura al mutare delle esigenze di contrasto, nel rispetto del principio di stretta necessità della limitazione del diritto alla privacy rispetto all'obiettivo del contrasto di reati gravi. La Corte precisa, infine, che l'eventuale difficoltà che uno Stato possa incontrare nel

definire presupposti e limiti della conservazione mirata non può giustificare la previsione della conservazione generalizzata e indifferenziata dei tabulati, che da eccezione diverrebbe in tal modo regola.

Per quanto, invece, concerne la conservazione rapida dei tabulati dei quali i fornitori dispongano a fini commerciali (tecnici o di fatturazione), la Corte ammette che la legislazione nazionale ne preveda- a fini di contrasto di forme gravi di criminalità o per esigenze di sicurezza nazionale- la conservazione, per un periodo determinato, sulla base di un provvedimento dell'autorità competente "soggetto a un controllo giurisdizionale effettivo". In tal caso, l'ordine di conservazione può estendersi, pur nella misura della stretta necessità, ai tabulati relativi a persone diverse "*da quelle sospettate di avere progettato o commesso un reato grave o un attentato alla sicurezza nazionale, purché tali dati possano contribuire, sulla base di elementi oggettivi e non discriminatori, all'accertamento di un siffatto reato o attentato alla sicurezza nazionale, quali i dati della vittima o del suo ambiente sociale o professionale*". Inoltre, l'ordine di conservazione rapida può riguardare anche zone geografiche determinate in connessione, a vario titolo, con il fatto di reato e può, in ogni caso, intervenire sin dall'avvio delle indagini (punti 90 e 91).

3. I riflessi sulla disciplina interna

Benché, appunto, la sentenza del 5 aprile non sia realmente innovativa, ma riprenda principi già affermati, in particolare con le sentenze Tele2 e La Quadrature du Net, la nettezza e la particolare articolazione con cui essi sono oggi esposti suggeriscono una riflessione sulla compatibilità della disciplina interna (peraltro recentemente riformata proprio a seguito della sentenza H.K. del 2 marzo 2021) con quella europea.

In linea generale, il massimo punto di tensione con i principi affermati dalla Corte riguarda l'oggetto della selezione richiesta per escludere la massività della misura. La disciplina interna si è strutturata, peraltro non da ora, sulla riferibilità del criterio selettivo al solo momento acquisitivo. In altri termini, il criterio della gravità del reato è stato concepito come idoneo a modulare diversamente la profondità cronologica dell'acquisizione processuale, senza tuttavia incidere ex ante sulla fase della conservazione. E' significativa, sul punto, la posizione espressa dalla sentenza 13 febbraio 2020, n. 5741 della Corte di Cassazione, secondo cui "non può ritenersi che la disciplina italiana di conservazione dei dati di traffico (c.d. *data retention*) sia in contrasto con le pronunce della Corte di giustizia datate 8 aprile 2014 e 21 dicembre 2016 poiché la

suddetta normativa prevede la conservazione dei dati per un periodo limitato pari a 24 mesi*, subordina la possibilità di acquisizione degli stessi soltanto per finalità di accertamento e repressione dei reati,* prevede che l'utilizzazione degli stessi dati sia sottoposta al provvedimento di acquisizione emesso da parte del Pubblico Ministero e cioè di un organo giurisdizionale che procede nell'ambito di una attività di indagine preliminare. Ne deriva quindi affermare che la legislazione italiana *non prevede la facoltà delle autorità pubbliche di accesso indiscriminato ai dati sensibili bensì la limita ai soli casi di indagini per fatti di reato svolte entro un determinato arco temporale di 24 mesi* (elevati a 72 solo per fatti di reato di particolare allarme sociale) e la subordina alla autorizzazione proveniente da un organo giurisdizionale. [...] Va pertanto ribadita la legittimità della normativa nazionale di riferimento costituita dall'art. 132 Codice della privacy, poiché la deroga al diritto alla riservatezza delle comunicazioni è prevista per un periodo limitato, ha come esclusivo obiettivo l'accertamento e la repressione dei reati è subordinato alla emissione di un provvedimento da parte di un'autorità giurisdizionale" (c.a.).

La soluzione interna è certamente coerente con la natura "retrospettiva" di questo mezzo di ricerca della prova, che presuppone una conservazione indistinta in vista di un'acquisizione solo eventuale. Inoltre, essa riflette – e rifletteva anche sul punto, poi modificato con il d.l. 132 del 2021, dell'attribuzione al solo pubblico ministero della potestà acquisitiva – la posizione tenuta dalla Corte costituzionale in relazione alla diversa ingerenza, sulla privacy, della *data retention*, rispetto a quella propria delle intercettazioni, tale da giustificarne la differente disciplina.

In linea con la teoria tedesca delle "sfere" concentriche lungo le quali si articolerebbe, con diversa intensità, la tutela dei diritti fondamentali, già con la sentenza n. 81 del 1993, la Consulta ha ravvisato nell'acquisizione dei tabulati un'incidenza solo marginale sul diritto alla libertà e segretezza delle comunicazioni di cui all'art. 15 Cost. Come sottolinea Carlotta Conti (Sicurezza e riservatezza, in *Dir.pen.proc*., 2019, n. 11, 1572), infatti, la natura emergente o periferica del diritto inciso è il parametro che induce la Corte a ritenere, secondo i principi di adeguatezza e proporzionalità, sufficiente un modello di tutela più tenue. La Corte allora delineava, dunque, parallelamente alle prove incostituzionali (e come tali inammissibili) perché, appunto, lesive di diritti costituzionalmente tutelati, la categoria delle prove (allora atipiche) "rafforzate" perché incisive su diritti di libertà, ammettendo per lesioni solo periferiche di tali diritti un bilanciamento "attenuato" che moduli le tutele in ragione dell'entità solo marginale della compressione del diritto.

Quest'impianto, pur ragionevole, mal si concilia ora con la posizione della Corte di giustizia, che muove dalla considerazione dell'impatto significativo della data retention sulla riservatezza

individuale e, peraltro, di tutti i cittadini (nell'ipotesi, appunto, di una conservazione generalizzata, preventiva e indifferenziata) a prescindere da alcuna connessione con possibili reati.

La disciplina interna che- pur a fronte di una differenziazione per titolo di reato in fase acquisitiva presuppone, comunque, la conservazione preventiva e generalizzata dei dati di traffico relativo alla generalità indistinta dei cittadini – sembra dunque da rivedere nel suo impianto complessivo, almeno con riferimento ad alcune tipologie di dati.

Da un lato, andrà probabilmente operata una distinzione fondata sulla tipologia dei dati, con un regime differenziato e meno rigido per quelli relativi all'identità civile degli utenti dei mezzi di comunicazione elettronica e agli indirizzi IP attribuiti alla fonte di una connessione.

Dall'altro lato, sarà opportuno disciplinare i parametri, soggettivi, spaziali e se del caso di altra natura (purché, appunto, oggettiva e non discriminatoria) sulla base dei quali procedere alla conservazione mirata dei dati di traffico e relativi all'ubicazione da utilizzare a fini di contrasto di gravi reati (categoria suscettibile probabilmente di estendersi anche oltre quella dei delitti di competenza delle Procure distrettuali). Nella delineazione dei criteri di ordine soggettivo, sarà certamente da evitare ogni previsione suscettibile di far riemergere logiche da "tipo di autore" che rappresenterebbe l'esito paradossale di affermazioni, quali quelle della Corte di giustizia, mosse certamente da obiettivi diversi.

Per altro aspetto, diverrà tanto più opportuno disciplinare positivamente la cd conservazione rapida e il relativo accesso, definendo presupposti e modalità per l'attuazione tempestiva dell'ordine di quick freeze o, direttamente, di acquisizione dei dati, ipotizzando eventualmente anche procedimenti di convalida di ordini adottati d'urgenza al fine di impedire che il decorso del periodo massimo di memorizzazione per fini commerciali vanifichi elementi di prova.

Così come sarà opportuno chiarire- proprio alla luce della specifica differenza che emerge dalla sentenza tra la conservazione preventiva e generalizzata dei dati di traffico relativi alla generalità indistinta dei cittadini e l'acquisizione del dato relativo al traffico all'interno del singolo processo, accedendo a dati conservati in supporti nella disponibilità dell'a.g.- come quest'ultimo tema esuli dalla problematica affrontata dalla Corte.

Per quanto, infine, concerne la conservazione dei tabulati ai sensi dell'art. 4 d.l. 144 del 2005, convertito con modificazioni dalla l. 155 del 2005, essa, in quanto funzionale a fini di sicurezza nazionale, sembra riconducibile alla sfera di legittimità delineata dalla Corte di giustizia. Si potrebbe tuttavia riflettere sull'opportunità di una giurisdizionalizzazione piena anche di questo

procedimento acquisitivo. La competenza del Procuratore generale presso la Corte d'appello di Roma potrebbe, infatti ritenersi non del tutto in linea con l'esigenza del vaglio di un giudice o, comunque, di un'autorità indipendente ribadita dalla sentenza in commento, laddove si legga questo requisito alla luce dell'esigenza di terzietà richiesta, per l'organo titolare del potere autorizzatorio, dalla pronuncia H.K. del 2 marzo 2021. Analoga giurisdizionalizzazione piena potrebbe, peraltro, essere prevista per la diversa ipotesi di conservazione, essa sì, rapida di cui all'articolo 132, c.4-ter d.lgs. 196 del 2003 e s.m.i.,

Resta, però, da riflettere sulla ragionevolezza di una distinzione così significativa (in termini di strumenti investigativi esperibili) tra *data retention* funzionale ad esigenze di tutela della sicurezza nazionale e conservazione a "fini di giustizia"; distinzione certamente assai approfondita dalla sentenza in esame.

[1] L'esigenza di piena giurisdizionalizzazione della procedura di acquisizione dei tabulati è stata valorizzata, dal legislatore interno, con il d.l. 132 del 2021, convertito, con modificazioni, dalla l. 178 del 2021. La sentenza della Corte e il decreto-legge sono stati pubblicati e commentati su questa Rivista. La disciplina transitoria introdotta dall'art. 1, comma 1-bis, della legge di conversione del d.l. 132- che ha consentito l'utilizzazione dei dati relativi al traffico telefonico, al traffico telematico e alle chiamate senza risposta acquisiti nei procedimenti penali in data antecedente all'entrata in vigore della riforma- è stata, peraltro, ritenuta compatibile con l'art. 15, par. 1, della Direttiva 2002/58/CE "in quanto, in un'ottica di ragionevole ed equilibrato contemperamento di interessi diversi, persegue la finalità di non disperdere dati già acquisiti, subordinandone l'utilizzazione alla significativa illiceità penale di predeterminate ipotesi per cui è consentita l'acquisizione a regime e alla sussistenza di "altri elementi di prova", quale requisito di compensazione della mancanza di un provvedimento giudiziale di autorizzazione all'acquisizione stessa " dalla Terza sezione penale della Corte di cassazione, con sent. n. 11991 del 31/01/2022 (dep. 01/04/2022).

[2] In particolare al punto 156 de La Quadrature du Net, secondo cui "*solo la lotta alle forme gravi di criminalità e la prevenzione delle minacce gravi alla sicurezza pubblica sono idonee, al pari della salvaguardia della sicurezza nazionale, a giustificare siffatta ingerenza. Inoltre, la durata della conservazione non può eccedere quella strettamente necessaria alla luce dell'obiettivo perseguito. Infine, una misura di questa natura deve prevedere condizioni e garanzie rigorose riguardo all'utilizzo di tali dati, segnatamente mediante tracciamento, in relazione alle comunicazioni ed attività effettuate online dagli interessati*".