Trattamento dei dati personali nel settore delle comunicazioni elettroniche. La Corte di Giustizia si pronuncia sui limiti della conservazione generalizzata ed indifferenziata dei dati di traffico e di ubicazione

11/02/2021

DIRITTO EUROPEO E DELLA CONCORRENZA, PROTEZIONE DEI DATI E CYBERSECURITY, CONTENZIOSO

Roberto A. Jacchia
Marco Stillo

In data 6 ottobre 2020, la Corte di Giustizia dell'Unione Europea si è pronunciata nelle Cause Riunite C-511/18, C-512/18 e C-520/18, *La Quadrature du Net e a. contro Premier ministre e a.*, sull'interpretazione dell'articolo 15, paragrafo 1, della Direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche[1], e degli articoli da 12 a 15 della Direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il

[1] GUUE L 201 del 31.07.2002.

commercio elettronico, nel mercato interno[2], letti alla luce degli articoli 4, da 6 a 8 e 11 e dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione nonché dell'articolo 4, paragrafo 2, del Trattato sull'Unione Europea (TUE). Tali cause sono state discusse in parallelo alla causa *Privacy International* sempre del 2020, in cui la Corte si è del pari pronunciata sulla riservatezza delle comunicazioni elettroniche e sulla salvaguardia della sicurezza nazionale[3].

Si tratta di una sentenza particolarmente complessa, il cui effetto netto è di porre dei limiti di legalità, di proporzionalità e, in ultima analisi, di funzionamento dello Stato di diritto negli ordinamenti democratici, all'acquisizione generalizzata e all'utilizzo dei dati estraibili dalle comunicazioni elettroniche, finanche in contesti di protezione della sicurezza nazionale, e di lotta al terrorismo e alla criminalità.

La domanda di pronuncia pregiudiziale nella Causa C-511/18 era stata presentata nell'ambito di controversie tra, da un lato, la *Quadrature du Net*, la *French Data Network*, la *Fédération des fournisseurs d'accès à Internet associatifs* e la *Igwan.net* e, dall'altro, il *Premier ministre* (Primo ministro francese), il *Garde des Sceaux, ministre de la Justice* (Ministro guardasigilli della Giustizia francese), il *ministre de l'Intérieur* (Ministro dell'Interno francese) e il *ministre des Armées* (Ministro delle Forze armate francese) francesi, in merito alla legittimità di diversi decreti relativi ai servizi di informazione[4]. Più particolarmente, le ricorrenti nel giudizio principale sostenevano che tali atti violassero la Costituzione francese, la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU) nonché le Direttive 2000/31 e 2002/58, lette alla luce degli articoli 7, 8 e 47 della Carta. Di talché, esse avevano adito il *Conseil d'État* (Consiglio di Stato francese; "giudice del rinvio") che, alla luce della necessità di interpretare la normativa europea rilevante in materia, aveva deciso di sospendere il procedimento e di sottoporre alla Corte di Giustizia tre questioni pregiudiziali.

La domanda nella Causa C-512/18 era stata presentata nell'ambito di controversie tra, da un lato, la *French Data Network*, la *Quadrature du Net* e la *Fédération des fournisseurs d'accès à Internet associatifs* e, dall'altro, il Primo ministro e il Ministro della Giustizia francesi in merito alla legittimità dell'articolo R. 10-13 del *code des postes et des communications électroniques* (codice delle poste e delle comunicazioni

[2] GUUE L 178 del 17.07.2000.
[3] CGUE 06.10.2020, Causa C-623/17, *Privacy International contro Secretary of State for Foreign and Commonwealth Affairs e a*. Per ulteriori informazioni si veda il nostro precedente contributo, disponibile al seguente LINK.
[4] Nello specifico, si trattava del *décret n.°2015-1185, du 28 septembre 2015, portant désignation des services spécialisés de renseignement* (decreto n. 2015/1185, del 28 settembre 2015, recante designazione dei servizi d'informazione specializzati), del *décret n° 2015-1211, du 1er octobre 2015, relatif au contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État* (decreto n. 2015-1211, del 1° ottobre 2015, relativo al contenzioso in materia di attuazione delle tecniche di informazione soggette ad autorizzazione e di fascicoli concernenti la sicurezza dello Stato), del *décret n. 2015-1639, du 11 décembre 2015, relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure* (decreto n. 2015-1639, dell'11 dicembre 2015, relativo alla designazione dei servizi diversi dai servizi di informazione specializzati, autorizzati a utilizzare le tecniche di cui al titolo V del libro VIII del codice della sicurezza interna, adottato in applicazione dell'articolo L. 811-4 del codice della sicurezza interna) nonché del *décret n. 2016-67, du 29 janvier 2016, relatif aux techniques de recueil de renseignement* (decreto n. 2016-67, del 29 gennaio 2016, in materia di tecniche di raccolta di informazioni).

elettroniche; CPCE)[5] e del *décret n. 2011-219, du 25 février 2011, relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne* (decreto n. 2011-219, del 25 febbraio 2011, sulla conservazione dei dati che consentono l'identificazione di chiunque abbia contribuito alla creazione di un contenuto offerto *online*). Ritenendo tali disposizioni contrarie all'articolo 15, paragrafo 1, della Direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 della Carta, le ricorrenti avevano adito il Consiglio di Stato francese, che aveva anche in quel caso deciso di sospendere il procedimento e di sottoporre alla Corte di Giustizia due questioni pregiudiziali.

Infine, la domanda nella Causa C-520/18 era stata presentata nell'ambito di controversie tra, da un lato, l'*Ordre des barreaux francophones et germanophone*, l'*Académie Fiscale ASBL*, *UA*, la *Liga voor Mensenrechten ASBL* e la *Ligue des droits de l'Homme ASBL, VZ, WY e XX* e, dall'altro, il *Conseil des ministres* (Consiglio dei ministri) belga in merito alla legittimità della *loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques* (legge del 29 maggio 2016 sulla raccolta e conservazione dei dati nel settore delle comunicazioni elettroniche). Più particolarmente, le ricorrenti avevano prospettato che tale legge violasse gli articoli 10 e 11 della Costituzione belga, letta in combinato disposto con gli articoli 5, da 6 a 11, 14, 15, 17 e 18 della CEDU, gli articoli 7, 8, 11 e 47 nonché l'articolo 52, paragrafo 1, della Carta, l'articolo 17 del Patto internazionale relativo ai diritti civili e politici, i principi generali di certezza del diritto, di proporzionalità e di autodeterminazione in materia di informazione nonché l'articolo 5, paragrafo 4, TUE. Esse avevano adito la *Cour constitutionnelle* (Corte costituzionale belga; "giudice del rinvio"), che aveva sospeso il procedimento e sottoposto alla Corte di Giustizia tre questioni pregiudiziali.

Riuniti i procedimenti, la Corte ha deciso di esaminare in primo luogo le prime questioni nelle Cause C-511/18 e C-512/18 nonché le questioni prima e seconda nella Causa C-520/18, con le quali i giudici del rinvio avevano chiesto di conoscere se l'articolo 15, paragrafo 1[6], della Direttiva 2002/58 debba essere

[5] L'articolo R. 10-13 del CPCE dispone: "*... In applicazione dell'articolo L. 34-1, paragrafo III, gli operatori di comunicazione elettronica conservano, ai fini dell'indagine, dell'accertamento e del perseguimento dei reati:*
a) le informazioni che permettono di identificare l'utente;
b) i dati relativi alle apparecchiature terminali di comunicazione utilizzate;
c) le caratteristiche tecniche nonché la data, l'ora e la durata di ogni comunicazione;
d) i dati relativi ai servizi complementari richiesti o utilizzati e i loro fornitori;
e) i dati che consentono di identificare il destinatario o i destinatari della comunicazione.
Nel caso delle attività di telefonia, l'operatore conserva i dati di cui al paragrafo II e, inoltre, i dati che consentono di identificare l'origine e l'ubicazione della comunicazione.
I dati di cui al presente articolo sono conservati per un periodo di un anno a decorrere dalla data della loro registrazione.
I costi supplementari identificabili e specifici sostenuti dagli operatori ai quali le autorità giudiziarie hanno ordinato di fornire dati rientranti nelle categorie menzionate nel presente articolo sono compensati con le modalità previste all'articolo R. 213-1 del code de procédure pénale...".

[6] L'articolo 15 della Direttiva 2002/58, intitolato "Applicazione di alcune disposizioni della direttiva 95/46/CE", al paragrafo 1 dispone: "*... 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*

interpretato nel senso che osta ad una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica, ai fini previsti da tale articolo, una conservazione generalizzata e indifferenziata dei dati relativi al traffico e di quelli relativi all'ubicazione.

La Corte ha preliminarmente ricordato che l'articolo 15, paragrafo 1, letto in combinato disposto con l'articolo 3[7], della Direttiva 2002/58 deve essere interpretato nel senso che rientra nell'ambito di applicazione della direttiva non soltanto una misura legislativa che impone ai fornitori di servizi di comunicazione elettronica di conservare i dati relativi al traffico e quelli relativi all'ubicazione, e bensì anche una misura che impone loro di accordare alle autorità nazionali competenti l'accesso a tali dati, in quanto misure legislative di tal genere implicano necessariamente un trattamento di questi dati e non possono, in quanto disciplinano anche le attività degli stessi fornitori, essere considerate come attività caratteristiche degli Stati[8]. Inoltre, un'interpretazione della Direttiva 2002/58 secondo cui le disposizioni del suo articolo 15, paragrafo 1, sarebbero escluse dal suo ambito di applicazione, in quanto le finalità che tali disposizioni devono soddisfare coincidono sostanzialmente con quelle perseguite dalle attività contemplate dall'articolo 1, paragrafo 3[9], della medesima direttiva, priverebbe l'articolo in questione di qualsiasi effetto utile[10]. Di talché, la nozione di "*attività*" di cui all'articolo 1, paragrafo 3, della Direttiva 2002/58 non può essere interpretata nel senso che comprende le disposizioni legislative menzionate all'articolo 15, paragrafo 1, di tale direttiva.

Questa conclusione non viene inficiata dalle disposizioni dell'articolo 4, paragrafo 2[11], TUE. Sebbene, infatti, spetti agli Stati Membri definire i loro interessi essenziali in materia di sicurezza e decidere le misure idonee a garantirla sia all'interno che all'estero, la mera circostanza che una misura nazionale sia stata adottata a tali fini non può comportare l'inapplicabilità del diritto europeo e dispensare gli Stati Membri dal suo rispetto[12]. Quando, invece, gli Stati Membri adottano direttamente misure che derogano alla riservatezza delle comunicazioni elettroniche, senza

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...".

[7] L'articolo 3 della Direttiva 2002/58, intitolato "Servizi interessati", dispone: "*... La presente direttiva si applica al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nella Comunità.*
Gli articoli 8, 10 e 11 si applicano alle linee di abbonati collegate a centrali telefoniche digitali e, qualora sia tecnicamente possibile e non richieda un onere economico sproporzionato, alle linee di abbonati collegate a centrali telefoniche analogiche.
Gli Stati membri notificano alla Commissione i casi in cui l'osservanza delle prescrizioni di cui agli articoli 8, 10 e 11 risulti tecnicamente impossibile o richieda un onere economico sproporzionato...".

[8] CGUE 02.10.2018, Causa C-207/16, *Ministerio Fiscal*, punti 35 e 37.

[9] L'articolo 1 della Direttiva 2002/58, intitolato "Finalità e campo d'applicazione", al paragrafo 3 dispone: "*... 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...*".

[10] CGUE 21.12.2016, Cause riunite C-203/15 e C-698/15, *Tele2*, punti 72-73.

[11] L'articolo 4 TUE al paragrafo 2 dispone: "*... L'Unione rispetta l'uguaglianza degli Stati membri davanti ai trattati e la loro identità nazionale insita nella loro struttura fondamentale, politica e costituzionale, compreso il sistema delle autonomie locali e regionali. Rispetta le funzioni essenziali dello Stato, in particolare le funzioni di salvaguardia dell'integrità territoriale, di mantenimento dell'ordine pubblico e di tutela della sicurezza nazionale. In particolare, la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro...*".

[12] CGUE 02.04.2020, Cause riunite C-715/17, C-718/17 e C-719/17, *Commissione/Polonia, Ungheria e Repubblica ceca (Meccanismo temporaneo di ricollocazione di richiedenti protezione internazionale)*, punti 143 e 170; CGUE 20.03.2018, Causa C-187/16, *Commissione/Austria (Tipografia di Stato)*, punti 75-76; CGUE 04.06.2013, Causa C-300/11, *ZZ*, punto 38.

imporre obblighi di trattamento ai fornitori di servizi che le gestiscono, la tutela dei dati delle persone interessate rientra non già nell'ambito di applicazione della Direttiva 2002/58, e bensì in quello del solo diritto nazionale, fatta salva l'applicazione della Direttiva (UE) 2016/680[13]. Di conseguenza, secondo la Corte, una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica di conservare dati relativi al traffico e dati relativi all'ubicazione a fini di salvaguardia della sicurezza nazionale e di lotta alla criminalità rientra nell'ambito di applicazione della Direttiva 2002/58.

Peraltro, nonostante l'articolo 15, paragrafo 1, della Direttiva 2002/58 consenta agli Stati Membri di introdurre eccezioni all'obbligo di garantire la riservatezza dei dati personali[14], nonché ai corrispondenti obblighi menzionati nei suoi articoli 6[15] e 9[16], tale facoltà non può giustificare che una deroga ai suddetti diritti ed obblighi diventi la regola[17]. Più particolarmente, l'elenco degli obiettivi di cui all'articolo 15, paragrafo 1, prima frase, della Direttiva 2002/58 ha carattere tassativo, di modo che le misure legislative nazionali adottate al riguardo debbono riflettere in modo effettivo e rigoroso almeno uno di essi[18]. Gli Stati Membri, inoltre, sono autorizzati ad adottare disposizioni legislative intese a limitare la portata dei diritti e degli obblighi di cui agli articoli 5, 6 e 9 di tale direttiva soltanto nel rispetto dei principi generali del diritto dell'Unione, tra i quali figura il principio di proporzionalità, e dei diritti fondamentali garantiti dalla Carta. A tal riguardo, l'obbligo imposto da uno Stato Membro ai fornitori di servizi di comunicazione elettronica in forza di una

[13] 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, *GUUE L 119 del 04.05.2016.*

[14] L'articolo 5 della Direttiva 2002/58, intitolato "Riservatezza delle comunicazioni", al paragrafo 1 dispone: "*... 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 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...*".

[15] L'articolo 6 della Direttiva 2002/58, intitolato "Dati sul traffico", ai paragrafi 1-2 dispone: "*... I dati sul traffico relativi agli abbonati ed agli utenti, trattati e memorizzati dal fornitore di una rete pubblica o di un servizio pubblico di comunicazione elettronica devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione di una comunicazione, fatti salvi i paragrafi 2, 3 e 5 del presente articolo e l'articolo 15, paragrafo 1.*
I dati relativi al traffico che risultano necessari ai fini della fatturazione per l'abbonato e dei pagamenti di interconnessione possono essere sottoposti a trattamento. Tale trattamento è consentito solo sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento...".

[16] L'articolo 9 della Direttiva 2002/58, intitolato "Dati relativi all'ubicazione diversi dai dati relativi al traffico", al paragrafo 1 dispone: "*... Se i dati relativi all'ubicazione diversi dai dati relativi al traffico, relativi agli utenti o abbonati di reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico possono essere sottoposti a trattamento, essi possono esserlo soltanto a condizione che siano stati resi anonimi o che l'utente o l'abbonato abbiano dato il loro consenso, e sempre nella misura e per la durata necessaria per la fornitura di un servizio a valore aggiunto. Prima di chiedere il loro consenso, il fornitore del servizio deve informare gli utenti e gli abbonati sulla natura dei dati relativi all'ubicazione diversi dai dati relativi al traffico che saranno sottoposti a trattamento, sugli scopi e sulla durata di quest'ultimo, nonché sull'eventualità che i dati siano trasmessi ad un terzo per la prestazione del servizio a valore aggiunto. Gli utenti e gli abbonati devono avere la possibilità di ritirare il loro consenso al trattamento dei dati relativi all'ubicazione diversi dai dati relativi al traffico in qualsiasi momento...*".

[17] CGUE 21.12.2016, Cause riunite C-203/15 e C-698/15, *Tele2*, punti 89 e 104.

[18] CGUE 02.10.2018, Causa C-207/16, *Ministerio Fiscal*, punto 52.

normativa nazionale, di conservare i dati di traffico al fine di renderli, se del caso, accessibili alle autorità nazionali competenti solleva questioni riguardanti il rispetto non soltanto degli articoli 7[19] e 8[20] della Carta, relativi, rispettivamente, alla tutela della vita privata e alla protezione dei dati personali, e bensì anche dell'articolo 11[21], relativo alla libertà di espressione[22].

La conservazione dei dati di traffico e di quelli relativi all'ubicazione degli utenti costituisce, di per sé, non solo una deroga al divieto, per qualsiasi persona diversa dagli utenti stessi, di memorizzare tali dati, e bensì anche un'ingerenza nei diritti fondamentali al rispetto della vita privata, a prescindere dalla circostanza che le informazioni relative a quest'ultima abbiano o meno un carattere sensibile o che gli interessati abbiano o meno subito eventuali inconvenienti in seguito a siffatta ingerenza[23]. Tali dati, infatti, possono rivelare informazioni su un numero significativo di aspetti della vita privata degli interessati, consentendo di trarre conclusioni in merito, tra le altre cose, alle abitudini della vita quotidiana, ai luoghi di soggiorno permanenti o temporanei, agli spostamenti nonché alle relazioni sociali, al tempo stesso fornendo gli strumenti per stabilirne un profilo alquanto preciso[24]. Di conseguenza, la conservazione dei dati relativi di e di quelli relativi all'ubicazione a fini di polizia è, di per sé, idoneo a ledere il diritto al rispetto delle comunicazioni e a comportare effetti dissuasivi sull'esercizio, da parte degli utenti, dei mezzi di comunicazione elettronica della loro libertà di espressione[25], potendo comportare rischi di abuso e di accesso illecito. Per tali ragioni, l'articolo 15, paragrafo 1, della Direttiva 2002/58 comporta che i diritti sanciti dagli articoli 7, 8 e 11 della Carta non si atteggino a prerogative assolute, e siano invece da considerarsi alla luce della loro funzione sociale[26], e pertanto, la sua interpretazione alla luce della Carta richiede che si tenga conto allo stesso modo dell'importanza dei diritti sanciti agli articoli 3, 4, 6 e 7 della stessa e di quella degli obiettivi di salvaguardia della sicurezza nazionale e di lotta alle forme gravi di criminalità nel contribuire alla protezione dei diritti e delle libertà altrui.

La tutela del diritto fondamentale al rispetto della vita privata esige che le deroghe e le restrizioni alla tutela dei dati personali operino entro i limiti dello stretto necessario. Un obiettivo di interesse generale, inoltre, non può essere perseguito senza tener conto del fatto che esso deve essere conciliato con i diritti fondamentali interessati dalla

[19] L'articolo 7 della Carta, intitolato "Rispetto della vita privata e della vita familiare", dispone: "*... Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni...*"
[20] L'articolo 8 della Carta, intitolato "Protezione dei dati di carattere personale", dispone: "*... 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 e 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...".
[21] L'articolo 11 della Carta, intitolato "Libertà di espressione e d'informazione", dispone: "*... 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.*
La libertà dei media e il loro pluralismo sono rispettati...".
[22] CGUE 21.12.2016, Cause riunite C-203/15 e C-698/15, *Tele2*, punti 91-92; CGUE 08.04.2014, Cause riunite C-293/12 e C-594/12 *Digital Rights*, punti 25 e 70.
[23] Parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, punti 124 e 126.
[24] CGUE 21.12.2016, Cause riunite C-203/15 e C-698/15, *Tele2*, punto 99; CGUE 08.04.2014, Cause riunite C-293/12 e C-594/12 *Digital Rights*, punto 27.
[25] CGUE 21.12.2016, Cause riunite C-203/15 e C-698/15, *Tele2*, punto 101; CGUE 08.04.2014, Cause riunite C-293/12 e C-594/12 *Digital Rights*, punto 28.
[26] CGUE 16.07.2020, Causa C-311/18, *Facebook Ireland e Schrems*, punto 172.

misura, effettuando un contemperamento equilibrato tra, da un lato, l'obiettivo di interesse generale e, dall'altro, i diritti di cui trattasi[27]. Più particolarmente, la possibilità per gli Stati Membri di giustificare una limitazione dei diritti e degli obblighi previsti agli articoli 5, 6 e 9 della Direttiva 2002/58 deve essere valutata guardando alla gravità dell'ingerenza che la restrizione comporta e verificando che l'importanza dell'obiettivo di interesse generale perseguito sia commisurata a detta gravità[28]. Nello specifico, per soddisfare il requisito di proporzionalità, debbono essere previste norme chiare e precise che disciplinino la portata e l'applicazione della misura e fissino una soglia minima di requisiti, di modo che le persone i cui dati personali sono oggetto di attenzione dispongano di garanzie sufficienti a proteggerli efficacemente dai rischi di abuso. Ne segue che una normativa che preveda forme di conservazione dei dati personali deve sempre rispondere a criteri oggettivi e a proporzionalità tra dati conservati e obiettivo perseguito[29].

L'importanza della salvaguardia della sicurezza nazionale, letta alla luce dell'articolo 4, paragrafo 2, TUE, supera quella della salvaguardia della sicurezza pubblica di cui all'articolo 15, paragrafo 1, della Direttiva 2002/58, in quanto attività idonee a destabilizzare le strutture costituzionali, politiche, economiche o sociali fondamentali di un Paese, si distinguono, per la loro natura e la loro particolare gravità, dal rischio generale di tensioni o perturbazioni, anche gravi, della pubblica sicurezza. In tali situazioni, pertanto, l'articolo 15, paragrafo 1, della Direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1[30], della Carta, non osta, in linea di principio, ad una misura legislativa che autorizzi le autorità competenti ad imporre ai fornitori di servizi di comunicazione elettronica di conservare i dati di traffico e di quelli relativi all'ubicazione degli utenti per un periodo limitato, se ricorrono circostanze sufficientemente concrete che consentono di ritenere che lo Stato Membro interessato affronti una minaccia grave alla sicurezza nazionale, attuale o fondatamente prevedibile.

Più particolarmente, un provvedimento che dispone la conservazione preventiva dei dati di tutti gli utenti dei mezzi di comunicazione elettronica deve essere temporalmente limitato allo stretto necessario, e non può superare un lasso di tempo prevedibile. La conservazione dei dati, inoltre, deve essere soggetta a limitazioni, ed accompagnarsi a garanzie rigorose che consentano di proteggere efficacemente gli interessati dal rischio di abusi, e non può avere carattere sistematico. Tenuto conto della gravità dell'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta risultante da misure di questo tipo, occorre, infine, garantire che il ricorso ad esse sia effettivamente limitato alle situazioni di minaccia grave per la sicurezza nazionale, con la conseguente necessità che il relativo provvedimento sia passibile di un controllo effettivo da parte di un giudice o di un organo amministrativo indipendente, la cui decisione sia dotata di efficacia vincolante, diretto ad accertare la sussistenza dei presupposti ed il rispetto delle condizioni e delle garanzie previste.

Conformemente al principio di proporzionalità, solo la lotta alle forme gravi di criminalità e la prevenzione di

[27] CGUE 08.04.2014, Cause riunite C-293/12 e C-594/12 *Digital Rights*, punto 52; CGUE 09.11.2010, Cause riunite C-92/09 e C-93/09, *Volker und Markus Schecke e Eifert*, punti 76-77 e 86; CGUE 16.12.2008, Causa C-73/07, *Satakunnan Markkinapörssi e Satamedia*, punto 56.
[28] CGUE 02.10.2018, Causa C-207/16, *Ministerio Fiscal*, punto 55.
[29] CGUE 03.10.2019, Causa C-70/18, *A e a.*, punto 63.
[30] L'articolo 52 della Carta, intitolato "Portata e interpretazione dei diritti e dei principi", al paragrafo 1 dispone: "*... 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...*".

minacce gravi alla sicurezza pubblica sono idonee a giustificare ingerenze gravi nei diritti fondamentali sanciti agli articoli 7 e 8 della Carta, come quelle che comporta la conservazione generalizzata dei dati di traffico e di ubicazione. Allo stesso modo, solo le ingerenze che non presentano un carattere grave possono essere giustificate da obiettivi di prevenzione, ricerca, accertamento e perseguimento dei reati in generale[31]. Una normativa nazionale che prevede la conservazione generalizzata e indifferenziata dei dati di traffico e di ubicazione, ai fini della lotta alle forme, anche gravi, di criminalità, pertanto, travalica i limiti dello stretto necessario e non può essere considerata giustificata in una società democratica, così come impone l'articolo 15, paragrafo 1, della Direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta[32]. Tenuto conto del carattere sensibile delle informazioni che possono fornire i dati in questione, infatti, la loro riservatezza è essenziale per il diritto al rispetto della vita privata, ed occorre che l'ingerenza costituisca, come prevede il sistema istituito dalla Direttiva 2002/58, l'eccezione e non la regola, e che i dati in questione non possano essere oggetto di politiche di conservazione sistematica e continuativa.

Anche gli obblighi positivi degli Stati Membri che possono derivare dagli articoli 3, 4 e 7 della Carta, e che riguardano l'introduzione di un assetto normativo che consenta una lotta effettiva alla criminalità, non possono giustificare ingerenze tanto gravi quanto quelle che comporta la conservazione generalizzata dei dati di traffico e di ubicazione della quasi totalità della popolazione, senza che i dati degli interessati siano idonei a rivelare una connessione, almeno indiretta, con l'obiettivo perseguito. Per contro, gli obiettivi di lotta alla criminalità grave, di prevenzione degli attentati gravi alla sicurezza pubblica e di salvaguardia della sicurezza nazionale sono idonei a giustificare, tenuto conto della loro importanza, l'ingerenza grave che comporta una conservazione mirata dei dati relativi di traffico e di ubicazione. Di conseguenza, l'articolo 15, paragrafo 1, della Direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, non osta a che uno Stato Membro adotti una normativa che consente, a titolo preventivo, una conservazione mirata dei dati relativi al traffico e di quelli relativi all'ubicazione degli utenti, per finalità di lotta conto la criminalità grave e di prevenzione delle minacce gravi alla sicurezza pubblica ed a fini di salvaguardia della sicurezza nazionale, a condizione che essa sia limitata allo stretto necessario per quanto concerne le categorie di dati da conservare, i mezzi di comunicazione e le persone interessate, e la durata della conservazione prevista[33].

Con la seconda e la terza questione nella Causa C-511/18, il giudice del rinvio aveva chiesto di conoscere se l'articolo 15, paragrafo 1, della Direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta, debba essere interpretato nel senso che osta ad una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica l'attuazione sulle loro reti di misure che consentano, da un lato, l'analisi automatizzata e la raccolta in tempo reale dei dati relativi al traffico e di quelli relativi all'ubicazione e, dall'altro, la raccolta in tempo reale dei dati tecnici relativi all'ubicazione delle apparecchiature terminali utilizzate, senza che sia prevista l'informazione delle persone interessate da tali trattamenti e operazioni di raccolta.

La Corte ha preliminarmente rilevato che una normativa nazionale come l'articolo L. 851-3 del *Code de la sécurité intérieure* (codice della sicurezza interna;

[31] CGUE 02.10.2018, Causa C-207/16, *Ministerio Fiscal*, punti 56-57; CGUE 21.12.2016, Cause riunite C-203/15 e C-698/15, *Tele2*, punto 102.
[32] CGUE 21.12.2016, Cause riunite C-203/15 e C-698/15, *Tele2*, punto 107.
[33] *Ibidem*, punto 108.

"CSI") francese[34], che autorizza il trattamento automatizzato dei dati relativi di traffico di ubicazione[35], non soltanto deroga all'obbligo di garantire la riservatezza delle comunicazioni elettroniche e dei dati correlati, e bensì costituisce un'ingerenza nei diritti fondamentali di cui agli articoli 7 e 8 della Carta, indipendentemente dall'uso ulteriore di tali dati, potendo anche produrre effetti dissuasivi sull'esercizio della libertà di espressione sancita dall'articolo 11 della Carta. Tale ingerenza, inoltre, appare particolarmente grave in quanto si applica globalmente a tutti coloro che si avvalgono dei mezzi di comunicazione elettronica e, di conseguenza, anche a coloro per quali non esiste alcun indizio tale da indurre a ritenere che il loro comportamento possa presentare un nesso con attività terroristiche.

Il requisito di cui all'articolo 52, paragrafo 1, della Carta, secondo cui qualsiasi limitazione all'esercizio dei diritti fondamentali deve essere prevista dalla legge, implica che la base giuridica che consente l'ingerenza in tali diritti debba definire essa stessa la portata della limitazione [36]. Inoltre, per soddisfare il requisito di proporzionalità, una normativa nazionale che disciplina l'accesso delle autorità ai dati di traffico e di ubicazione conservati non può limitarsi ad esigere che esso risponda ad una delle finalità perseguite dalla norma, e bensì deve prevedere anche le condizioni sostanziali e procedurali dell'utilizzo[37]. Nel caso concreto, l'ingerenza particolarmente grave che comporta una conservazione generalizzata e indifferenziata dei dati di traffico e di ubicazione, e quella costituita dal loro trattamento automatizzato, possono soddisfare il requisito di proporzionalità solo in situazioni nelle quali uno Stato Membro si trovi di fronte ad una minaccia grave, attuale o prevedibile alla sicurezza nazionale ed a condizione che la durata della conservazione sia limitata allo stretto necessario. Ne segue che, in tali situazioni, il trattamento automatizzato dei dati di traffico e di ubicazione di tutti gli utenti, per un periodo di tempo strettamente limitato, potrebbe essere giustificata con riguardo ai requisiti derivanti dall'articolo 15, paragrafo 1, della Direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta. Al fine di garantire che il ricorso ad una tale misura sia effettivamente limitato a quanto strettamente necessario per la salvaguardia della sicurezza nazionale, tuttavia, è essenziale che il provvedimento che autorizza il trattamento automatizzato possa formare oggetto di un controllo effettivo da parte di un giudice o di un organo amministrativo indipendente, la cui decisione sia dotata di effetto vincolante, allo scopo di verificare l'esistenza di una situazione che lo giustifichi, nel rispetto delle garanzie prescritte.

---

[34] L'articolo L. 851-3 del CSI al paragrafo 1 dispone: "*... Alle condizioni previste dal capo I del titolo II del presente libro ed esclusivamente al fine della prevenzione del terrorismo, può essere imposta agli operatori e ai soggetti menzionati all'articolo L. 851-1 l'attuazione sulle loro reti di trattamenti automatizzati destinati, in funzione di parametri specificati nell'autorizzazione, a individuare collegamenti in grado di rivelare una minaccia terroristica.*
Tali trattamenti automatizzati utilizzano esclusivamente le informazioni o i documenti previsti all'articolo L. 851-1, senza raccogliere dati diversi da quelli che rispondono ai loro parametri di progettazione e senza permettere l'identificazione delle persone alle quali si riferiscono le informazioni o i documenti.
Nel rispetto del principio di proporzionalità, l'autorizzazione del Primo ministro precisa l'ambito tecnico dell'attuazione di tali trattamenti...".

[35] Nello specifico, l'analisi automatizzata corrisponde ad un filtraggio di tutti i dati relativi al traffico e all'ubicazione conservati dai fornitori di servizi di comunicazione elettronica, effettuato da questi ultimi su richiesta delle autorità nazionali competenti e in applicazione dei parametri da queste stabiliti, di talché i dati degli utenti dei mezzi di comunicazione elettronica sono tutti verificati se corrispondono a tali parametri.

[36] CGUE 16.07.2020, Causa C-311/18, *Facebook Ireland e Schrems*, punto 175.

[37] Parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, punto 192.

A giudizio della Corte, una normativa nazionale che autorizza le raccolte di dati in tempo reale previste dall'articolo L. 851-2[38] e dall'articolo L. 851-4[39] del CSI deroga, al pari di quella che autorizza l'analisi automatizzata dei dati, all'obbligo di garantire la riservatezza delle comunicazioni elettroniche e dei dati correlati, costituendo anche un'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta e potendo comportare effetti dissuasivi sull'esercizio della libertà di espressione garantita dall'articolo 11 della Carta. Di conseguenza, nonostante l'obiettivo di prevenzione del terrorismo perseguito dal CSI sia idoneo a giustificare l'ingerenza che comporta la raccolta in tempo reale dei dati di traffico e di ubicazione, questa, a motivo del suo carattere particolarmente intrusivo, può essere attuata solo nei confronti delle persone rispetto alle quali sussiste un valido sospetto di implicazione in attività di terrorismo. Per contro, i dati delle persone che non rientrano in tale categoria possono essere oggetto soltanto di forme di accesso differito, che può avere luogo in situazioni particolari, come quelle riguardanti appunto le attività di terrorismo, e quando sussistano elementi oggettivi che consentano di ritenere che tali dati potrebbero, in un caso concreto, fornire un contributo effettivo alla lotta contro il terrorismo[40]. Un provvedimento che autorizza la raccolta in tempo reale dei dati di traffico e di ubicazione, inoltre, deve essere fondato su criteri oggettivi e non discriminatori previsti dalla legislazione nazionale, che deve definire le circostanze e le condizioni in presenza delle quali essa può venire autorizzata, potendo esserne interessate unicamente le persone che presentano un effettivo collegamento con l'obiettivo di prevenzione del terrorismo. L'attuazione di tale provvedimento, infine, deve essere subordinata al controllo preventivo di un giudice o di un organo amministrativo indipendente, la cui decisione sia provvista di effetto vincolante.

Con la seconda questione nella Causa C-512/18, il giudice del rinvio aveva domandato di conoscere se le disposizioni della Direttiva 2000/31[41], lette alla luce degli articoli da 6 a 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, debbano essere interpretate nel senso che ostano ad una normativa nazionale che impone ai fornitori di accesso a servizi di comunicazione al pubblico *online* e ai fornitori di servizi di *hosting* la conservazione generalizzata e indifferenziata, in particolare, dei dati personali relativi a tali servizi.

La Corte ha preliminarmente ricordato che, nonostante i servizi della società dell'informazione di cui all'articolo 2,

[38] L'articolo L. 851-2 del CSI dispone: "*... Alle condizioni previste al capo I del titolo II del presente libro ed esclusivamente al fine della prevenzione del terrorismo, può essere individualmente autorizzata la raccolta in tempo reale, sulle reti degli operatori e dei soggetti di cui all'articolo L. 851-1, delle informazioni o dei documenti previsti dal medesimo articolo L. 851-1 relativi a una persona precedentemente identificata come potenzialmente collegata a una minaccia. Qualora sussistano fondati motivi di ritenere che una o più persone appartenenti all'ambiente della persona interessata dall'autorizzazione possano fornire informazioni per la finalità che giustifica l'autorizzazione, quest'ultima può essere accordata anche individualmente per ciascuna di tali persone.*
Il numero massimo di autorizzazioni rilasciate in applicazione del presente articolo e simultaneamente in vigore è stabilito dal Primo ministro, previo parere della Commissione nazionale di controllo delle tecniche di informazione. La decisione che fissa tale contingente e la sua ripartizione tra i ministri menzionati all'articolo L. 821-2, primo comma, nonché il numero di autorizzazioni all'intercettazione rilasciate sono notificati alla Commissione...".

[39] L'articolo L. 851-4 del CSI dispone: "*... Alle condizioni previste dal capo I del titolo II del presente libro, i dati tecnici relativi all'ubicazione delle apparecchiature terminali utilizzate di cui all'articolo L. 851-1 possono essere raccolti su richiesta della rete e trasmessi in tempo reale dagli operatori ad un servizio del Primo ministro...*".

[40] CGUE 21.12.2016, Cause riunite C-203/15 e C-698/15, *Tele2*, punto 119.

[41] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno, GUUE L 178 del 17.07.2000.

lettera a)[42], della Direttiva 2000/31 comprendano quelli prestati a distanza mediante attrezzature elettroniche di trattamento e di memorizzazione di dati, quali i servizi di accesso a *internet* o ad una rete di comunicazione e servizi di *hosting*[43], le questioni connesse alla tutela della riservatezza delle comunicazioni e dei dati personali devono essere valutate alla luce della Direttiva 2002/58 e del Regolamento 2016/679[44]. Di conseguenza, l'obbligo imposto dall'articolo 6 della *loi n. 2004-575, du 21 juin 2004, pour la confiance dans l'économie numérique* (legge n. 2004-575, del 21 giugno 2004, per la fiducia nell'economia digitale; "LCEN") francese[45] ai fornitori di accesso a tali servizi *online* e di *hosting,* di conservare i relativi dati personali, deve essere valutato alla luce della Direttiva 2002/58 o del Regolamento 2016/679.

Per quanto riguarda, nello specifico, il Regolamento 2016/679, la Corte ha rilevato che l'articolo 23[46], al pari dell'articolo 15, paragrafo 1, della Direttiva 2002/58, consente agli Stati Membri di limitare, alla luce delle finalità da esso contemplate e mediante misure

[42] L'articolo 2 della Direttiva 2000/31, intitolato "Definizioni", alla lettera a) dispone: "*... Ai fini della presente direttiva valgono le seguenti definizioni: a) "servizi della società dell'informazione": i servizi ai sensi dell'articolo 1, punto 2, della direttiva 98/34/CE, come modificata dalla direttiva 98/48/CE...*".
[43] CGUE 07.08.2018, Causa C-521/17, *SNB-REACT*, punto 42; CGUE 15.09.2016, Causa C-484/14, *Mc Fadden*, punto 55; CGUE 16.02.2012, Causa C-360/10, *SABAM*, punto 34; CGUE 24.11.2011, Causa C-70/10, *Scarlet Extended*, punto 40.
[44] 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, *GUUE L 119 del 04.05.2016.*
[45] L'articolo 6 della LCEN al paragrafo 2 dispone: "*... Le persone di cui ai punti 1 e 2 del paragrafo I detengono e conservano i dati con modalità tali da permettere l'identificazione di chiunque abbia contribuito alla creazione del contenuto o di uno dei contenuti dei servizi da esse prestati...*".
[46] L'articolo 23 del Regolamento 2016/679, intitolato "Limitazioni", dispone: "*... Il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento può limitare, mediante misure legislative, la portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 e 34, nonché all'articolo 5, nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli da 12 a 22, qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare:*
a) la sicurezza nazionale;
b) la difesa;
c) la sicurezza pubblica;
d) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;
e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale;
f) la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari;
g) le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate; h) una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere da a), a e) e g);
i) la tutela dell'interessato o dei diritti e delle libertà altrui;
j) l'esecuzione delle azioni civili.
In particolare qualsiasi misura legislativa di cui al paragrafo 1 contiene disposizioni specifiche riguardanti almeno, se del caso:
a) le finalità del trattamento o le categorie di trattamento;
b) le categorie di dati personali;
c) la portata delle limitazioni introdotte;
d) le garanzie per prevenire abusi o l'accesso o il trasferimento illeciti;
e) l'indicazione precisa del titolare del trattamento o delle categorie di titolari;
f) i periodi di conservazione e le garanzie applicabili tenuto conto della natura, dell'ambito di applicazione e delle finalità del trattamento o delle categorie di trattamento;
g) i rischi per i diritti e le libertà degli interessati; e
h) il diritto degli interessati di essere informati della limitazione, a meno che ciò possa compromettere la finalità della stessa...".

legislative, la portata degli obblighi e dei diritti ivi previsti qualora tale limitazione sia necessaria e proporzionata in una società democratica per salvaguardare la finalità perseguita. Di conseguenza, tale articolo non può essere interpretato nel senso di conferire agli Stati Membri il potere di pregiudicare il rispetto della vita privata, in violazione dell'articolo 7 della Carta, nonché le altre garanzie previste da quest'ultima; pertanto, il potere da esso previsto può essere esercitato soltanto nel rispetto del principio di proporzionalità.

Con la terza questione nella Causa C-520/18, il giudice del rinvio aveva chiesto se un giudice nazionale possa applicare una disposizione del proprio diritto che lo autorizza a limitare nel tempo gli effetti di una dichiarazione di illegittimità ad esso incombente, in forza di tale diritto, nei riguardi di una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica, ai fini, tra l'altro, del perseguimento degli obiettivi di salvaguardia della sicurezza nazionale e di lotta alla criminalità, una conservazione generalizzata e indifferenziata dei dati di traffico e di ubicazione, in ragione della sua incompatibilità con l'articolo 15, paragrafo 1, della Direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta.

La Corte ha ricordato che il primato e l'applicazione uniforme del diritto dell'Unione[47] risulterebbero pregiudicati se i giudici degli Stati Membri avessero il potere di attribuire alle norme nazionali un rango preminente, anche solo provvisoriamente, in caso di contrasto[48]. Inoltre, a differenza delle vicende che avevano condotto alla pronuncia nella Causa C-411/17[49], una violazione dell'articolo 15, paragrafo 1, della Direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta, non potrebbe essere regolarizzata, in quanto il mantenimento degli effetti implicherebbe che ai fornitori di servizi di comunicazione elettronica continuino a venire imposti obblighi contrari al diritto dell'Unione e comportanti ingerenze gravi nei diritti fondamentali delle persone i cui dati sono stati conservati. DI talché, il giudice del rinvio non potrà applicare una disposizione del suo diritto nazionale che lo autorizza a limitare nel tempo gli effetti di una dichiarazione di illegittimità ad esso incombente in forza di tale diritto, con riguardo alla legislazione nazionale in questione.

Quanto, infine, all'interrogativo se il diritto dell'Unione osti all'utilizzo, nell'ambito di un procedimento penale, di informazioni ed elementi di prova ottenuti mediante una conservazione generalizzata e indifferenziata dei dati di traffico e di ubicazione incompatibile con tale diritto, la Corte ha osservato che, in assenza di una normativa europea in materia, spetta all'ordinamento interno di ciascuno Stato Membro stabilire le modalità processuali dei ricorsi intesi a garantire la tutela dei diritti spettanti ai singoli in forza del diritto dell'Unione, a condizione, tuttavia, che esse non siano meno favorevoli rispetto a quelle relative a situazioni analoghe assoggettate al diritto interno (principio di equivalenza) e che non rendano in pratica impossibile o eccessivamente difficile l'esercizio dei diritti conferiti dal diritto dell'Unione (principio di effettività)[50]. Di conseguenza, il principio di effettività impone al giudice nazionale di non tenere conto degli elementi di prova ottenuti mediante una conservazione generalizzata e indifferenziata dei dati di traffico e di

[47] CGUE 19.11.2019, Cause riunite C-585/18, C-624/18 e C-625/18, A.K. e a. (Indipendenza della Sezione disciplinare della Corte suprema), punti 157-160; CGUE 24.06.2019, Causa C-573/17, *Popławski*, punto 58; CGUE 22.06.2010, Cause riunite-188/10 e C-189/10, *Melki e Abdeli*, punto 43; CGUE 15.07.1964, Causa 6/64, *Costa*, pagg. 1143-1144

[48] CGUE 29.07.2019, Causa C-411/17, *Inter-Environnement Wallonie e Bond Beter Leefmilieu Vlaanderen*, punto 177.

[49] Si veda il punto 218 della sentenza.

[50] CGUE 19.12.2019, Causa C-752/18, *Deutsche Umwelthilfe*, punto 33; CGUE 24.10.2018, Causa C-234/17, *XC e a.*, punti 21-22; CGUE 06.10.2015, Causa C-69/14, *Târşia*, punti 26-27.

ubicazione incompatibile con il diritto dell'Unione, nell'ambito di un procedimento penale avviato nei confronti di persone sospettate di avere commesso atti di criminalità, qualora queste ultime non siano in grado di prendere efficacemente posizione su informazioni ed elementi di prova, provenienti da fonti che esulano dalla competenza del giudice adito e che potrebbero influenzare in maniera preponderante la valutazione dei fatti.

Roberto A. Jacchia

PARTNER

r.jacchia@dejalex.com

+39 02 72554.1

Via San Paolo 7
20121 - Milano

Marco Stillo

ASSOCIATE

m.stillo@dejalex.com

+32 (0)26455670

Chaussée de La Hulpe 187
1170 - Bruxelles

MILANO
Via San Paolo, 7 · 20121 Milano, Italia
T. +39 02 72554.1 · F. +39 02 72554.400
milan@dejalex.com

ROMA
Via Vincenzo Bellini, 24 · 00198 Roma, Italia
T. +39 06 809154.1 · F. +39 06 809154.44
rome@dejalex.com

BRUXELLES
Chaussée de La Hulpe 187 · 1170 Bruxelles, Belgique
T. +32 (0)26455670 · F. +32 (0)27420138
brussels@dejalex.com

MOSCOW
Ulitsa Bolshaya Ordynka 37/4 · 119017, Moscow, Russia
T. +7 495 792 54 92 · F. +7 495 792 54 93
moscow@dejalex.com