Raccolta della giurisprudenza

SENTENZA DELLA CORTE (Grande Sezione)

6 ottobre 2020*

[Testo rettificato con ordinanza del 16 novembre 2020]

Indice

* Lingua processuale: il francese.

«Rinvio pregiudiziale – Trattamento dei dati personali nel settore delle comunicazioni elettroniche – Fornitori di servizi di comunicazione elettronica – Fornitori di servizi di hosting e fornitori di accesso a Internet – Conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione – Analisi automatizzata dei dati – Accesso in tempo reale ai dati – Salvaguardia della sicurezza nazionale e lotta al terrorismo – Lotta alla criminalità – Direttiva 2002/58/CE – Ambito di applicazione – Articolo 1, paragrafo3, e articolo 3 – Riservatezza delle comunicazioni elettroniche – Tutela – Articolo 5 e articolo 15, paragrafo 1 – Direttiva 2000/31/CE – Ambito di applicazione – Carta dei diritti fondamentali dell'Unione europea – Articoli 4, da 6 a 8 e 11 e articolo 52, paragrafo 1 – Articolo 4, paragrafo 2, TUE»

Nelle cause riunite C-511/18, C-512/18 e C-520/18,

aventi ad oggetto le domande di pronuncia pregiudiziale proposte alla Corte, ai sensi dell'articolo 267 TFUE, dal Conseil d'État (Consiglio di Stato, Francia), con decisioni del 26 luglio 2018, pervenute in cancelleria il 3 agosto 2018 (C-511/18 e C-512/18), e dalla Cour constitutionnelle (Corte costituzionale, Belgio), con decisione del 19 luglio 2018, pervenuta in cancelleria il 2 agosto 2018 (C-520/18), nei procedimenti

La Quadrature du Net (C-511/18 e C-512/18),

French Data Network (C-511/18 e C-512/18),

Fédération des fournisseurs d'accès à Internet associatifs (C-511/18 e C-512/18),

Igwan.net (C-511/18),

contro

Premier ministre (C-511/18 e C-512/18),

Garde des Sceaux, ministre de la Justice (C-511/18 e C-512/18),

Ministre de l'Intérieur (C-511/18),

Ministre des Armées (C-511/18),

con l'intervento di:

Privacy International (C-512/18),

Center for Democracy and Technology (C-512/18),

e

Ordre des barreaux francophones et germanophone,

Académie Fiscale ASBL,

UA,

Liga voor Mensenrechten ASBL,

Ligue des Droits de l'Homme ASBL,

VZ,

WY,

XX

contro

Conseil des ministres,

con l'intervento di:

Child Focus (C-520/18),

LA CORTE (Grande Sezione),

composta da K. Lenaerts, presidente, R. Silva de Lapuerta, vicepresidente, J.-C. Bonichot, A. Arabadjiev, A. Prechal, M. Safjan, P.G. Xuereb e L.S. Rossi, presidenti di sezione, J. Malenovský, L. Bay Larsen, T. von Danwitz (relatore), C. Toader, K. Jürimäe, C. Lycourgos e N. Piçarra, giudici,

avvocato generale: M. Campos Sánchez-Bordona

cancelliere: C. Strömholm, amministratrice

vista la fase scritta del procedimento e in seguito alle udienze del 9 e 10 settembre 2019,

considerate le osservazioni presentate:

– per la Quadrature du Net, la Fédération des fournisseurs d'accès à Internet associatifs, la Igwan.net e il Center for Democracy and Technology, da A. Fitzjean Ò Cobhthaigh, avocat;

– per la French Data Network, da Y. Padova, avocat;

– per la Privacy International, da H. Roy, avocat;

– per l'Ordre des barreaux francophones et germanophone, da E. Kiehl, P. Limbrée, E. Lemmens, A. Cassart e J.-F. Henrotte, avocats;

– per l'Académie Fiscale ASBL e UA, da J.-P. Riquet,

– per la Liga voor Mensenrechten ASBL, da J. Vander Velpen, avocat;

– per la Ligue des Droits de l'Homme ASBL, da R. Jespers e J. Fermon, avocats;

– per VZ, WY e XX, da D. Pattyn, avocat;

– per la Child Focus, da N. Buisseret, K. De Meester e J. Van Cauter, avocats;

– per il governo francese, inizialmente da D. Dubois, F. Alabrune, D. Colas, E. de Moustier e A.-L. Desjonquères, successivamente da D. Dubois, F. Alabrune, E. de Moustier e A.-L. Desjonquères, in qualità di agenti;

– per il governo belga, da J.-C. Halleux, P. Cottin e C. Pochet, in qualità di agenti, assistiti da J. Vanpraet, Y. Peeters, S. Depré ed E. de Lophem, avocats;

– per il governo ceco, da M. Smolek, J. Vláčil e O. Serdula, in qualità di agenti;

– per il governo danese, inizialmente da J. Nymann-Lindegren, M. Wolff e P. Ngo, successivamente da J. Nymann-Lindegren e M. Wolff, in qualità di agenti;

– per il governo tedesco, inizialmente da J. Möller, M. Hellmann, E. Lankenau, R. Kanitz e T. Henze, successivamente da J. Möller, M. Hellmann, E. Lankenau e R. Kanitz, in qualità di agenti;

– per il governo estone, da N. Grünberg e A. Kalbus, in qualità di agenti;

– per il governo irlandese, da A. Joyce, M. Browne e G. Hodge, in qualità di agenti, assistiti da D. Fennelly, BL;

– per il governo spagnolo, inizialmente da L. Aguilera Ruiz e A. Rubio González, successivamente da L. Aguilera Ruiz, in qualità di agente;

– per il governo cipriota, da E. Neofytou, in qualità di agente;

– per il governo lettone, da V. Soņeca, in qualità di agente;

– per il governo ungherese, inizialmente da M.Z. Fehér e Z. Wagner, successivamente da M.Z. Fehér, in qualità di agente;

– per il governo dei Paesi Bassi, da M.K. Bulterman e M.A.M. de Ree, in qualità di agenti;

– per il governo polacco, da B. Majczyna, J. Sawicka e M. Pawlicka, in qualità di agenti;

– per il governo svedese, inizialmente da H. Shev, H. Eklinder, C. Meyer-Seitz e A. Falk, successivamente da H. Shev, H. Eklinder, C. Meyer-Seitz e J. Lundberg, in qualità di agenti;

– per il governo del Regno Unito, da S. Brandon, in qualità di agente, assistito da G. Facenna, QC, e da C. Knight, barrister;

– [trattino eliminato con ordinanza del 16 novembre 2020];

– per la Commissione europea, inizialmente da H. Kranenborg, M. Wasmeier e P. Costa de Oliveira, successivamente da H. Kranenborg e M. Wasmeier, in qualità di agenti;

– per il Garante europeo della protezione dei dati, da T. Zerdick e A. Buchta, in qualità di agenti,

sentite le conclusioni dell'avvocato generale, presentate all'udienza del 15 gennaio 2020,

ha pronunciato la seguente

Sentenza

1 Le domande di pronuncia pregiudiziale vertono sull'interpretazione, da un lato, dell'articolo 15, paragrafo 1, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa 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) (GU 2002, L 201, pag. 37), come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009 (GU 2009, L 337, pag. 11) (in prosieguo: la «direttiva 2002/58»), e, dall'altro, degli articoli da 12 a 15 della 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 («Direttiva sul commercio elettronico») (GU 2000, L 178, pag. 1), 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 europea (in prosieguo: la «Carta») nonché dell'articolo 4, paragrafo 2, TUE.

2 La domanda nella causa C-511/18 è stata presentata nell'ambito di controversie che oppongono la Quadrature du Net, la French Data Network, la Fédération des fournisseurs d'accès à Internet associatifs e la Igwan.net al Premier ministre (Primo ministro, Francia), al Garde des Sceaux, ministre de la Justice (Ministro guardasigilli della Giustizia, Francia), al ministre de l'Intérieur (Ministro dell'Interno, Francia) e al ministre des Armées (Ministro delle Forze armate, Francia) in merito alla

legittimità 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) (JORF del 29 settembre 2015, testo 1 di 97; in prosieguo: il «decreto n. 2015-1185»), 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) (JORF del 2 ottobre 2015, testo 7 di 108; in prosieguo: il «decreto n. 2015-1211»), 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) (JORF del 12 dicembre 2015, testo 28 di 127; in prosieguo: il «decreto n. 2015-1639»), 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) (JORF del 31 gennaio 2016, testo 2 di 113; in prosieguo: il «decreto n. 2016-67»).

3 La domanda nella causa C-512/18 è stata presentata nell'ambito di controversie che oppongono la French Data Network, la Quadrature du Net e la Fédération des fournisseurs d'accès à Internet associatifs al Primo ministro (Francia) e al Ministro guardasigilli della Giustizia (Francia) in merito alla legittimità dell'articolo R. 10-13 del code des postes et des communications électroniques (codice delle poste e delle comunicazioni elettroniche) (in prosieguo: il «CPCE») 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) (JORF del 1° marzo 2011, testo 32 di 170; in prosieguo: il «decreto n. 2011-219»).

4 La domanda nella causa C-520/18 è stata presentata nell'ambito di controversie che oppongono l'Ordre des barreaux francophones et germanophone, l'Académie Fiscale ASBL, UA, la Liga voor Mensenrechten ASBL, la Ligue des droits de l'Homme ASBL, VZ, WY e XX al Conseil des ministres (Consiglio dei ministri, Belgio) 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) (*Moniteur belge* del 18 luglio 2016, pag. 44717; in prosieguo: la «legge del 29 maggio 2016»).

Contesto normativo

Diritto dell'Unione

Direttiva 95/46

5 La 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, nonché alla libera circolazione di tali dati (GU 1995, L 281, pag. 31), è stata abrogata, a decorrere dal 25 maggio 2018, dal regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla tutela delle

persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46 (GU 2016, L 119, pag. 1). L'articolo 3, paragrafo 2, della direttiva 95/46 disponeva quanto segue:

«Le disposizioni della presente direttiva non si applicano ai trattamenti di dati personali:

– effettuati per l'esercizio di attività che non rientrano nel campo di applicazione del diritto comunitario, come quelle previste dai titoli V e VI del trattato sull'Unione europea e comunque ai trattamenti aventi come oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato, laddove tali trattamenti siano connessi a questioni di sicurezza dello Stato) e le attività dello Stato in materia di diritto penale;

– effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico».

6 L'articolo 22 della direttiva 95/46, contenuto nel capo III della stessa, intitolato «Ricorsi giurisdizionali, responsabilità e sanzioni», era così formulato:

«Fatti salvi ricorsi amministrativi che possono essere promossi, segnatamente dinanzi all'autorità di controllo di cui all'articolo 28, prima che sia adita l'autorità giudiziaria, gli Stati membri stabiliscono che chiunque possa disporre di un ricorso giurisdizionale in caso di violazione dei diritti garantitigli dalle disposizioni nazionali applicabili al trattamento in questione».

Direttiva 97/66

7 A termini dell'articolo 5 della 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 (GU 1997, L 24, pag. 1), intitolato «Riservatezza delle comunicazioni»:

«1. Gli Stati membri garantiscono mediante normative nazionali la riservatezza delle comunicazioni effettuate mediante la rete pubblica di telecomunicazione e i servizi di telecomunicazione offerti al pubblico. In particolare essi vietano l'ascolto, l'intercettazione, la memorizzazione o altri generi di intercettazione o di sorveglianza delle comunicazioni ad opera di persone diverse dagli utenti, senza il consenso di questi ultimi, eccetto quando sia autorizzato legalmente, a norma dell'articolo 14, paragrafo 1.

2. Il paragrafo [1] non riguarda la registrazione di comunicazioni legalmente autorizzata, nel quadro delle legittime prassi commerciali, allo scopo di fornire la prova di una transazione o di qualsiasi altra comunicazione commerciale».

Direttiva 2000/31

8 I considerando 14 e 15 della direttiva 2000/31 prevedono quanto segue:

«(14) La protezione dei singoli relativamente al trattamento dei dati personali è disciplinata unicamente dalla direttiva [95/46] e dalla direttiva [97/66], che sono integralmente applicabili ai servizi della società dell'informazione. Dette direttive già istituiscono un quadro giuridico comunitario nel campo della protezione dei dati personali e pertanto non è necessario includere tale aspetto nella presente direttiva per assicurare il buon funzionamento del mercato interno, in particolare la libera circolazione dei dati personali tra gli Stati membri. L'applicazione della presente direttiva deve essere pienamente conforme ai principi relativi alla protezione dei

dati personali, in particolare per quanto riguarda le comunicazioni commerciali non richieste e il regime di responsabilità per gli intermediari. La presente direttiva non può impedire l'utilizzazione anonima di reti aperte quali Internet.

(15) La riservatezza delle comunicazioni è assicurata dall'articolo 5 della direttiva [97/66]. In base a tale direttiva, gli Stati membri devono vietare qualsiasi forma di intercettazione o di sorveglianza non legalmente autorizzata di tali comunicazioni da parte di chi non sia il mittente o il destinatario».

9 L'articolo 1 della direttiva 2000/31 è così formulato:

«1. La presente direttiva mira a contribuire al buon funzionamento del mercato interno garantendo la libera circolazione dei servizi della società dell'informazione tra Stati membri.

2. La presente direttiva ravvicina, nella misura necessaria alla realizzazione dell'obiettivo di cui al paragrafo 1, talune norme nazionali sui servizi della società dell'informazione che interessano il mercato interno, lo stabilimento dei prestatori, le comunicazioni commerciali, i contratti per via elettronica, la responsabilità degli intermediari, i codici di condotta, la composizione extragiudiziaria delle controversie, i ricorsi giurisdizionali e la cooperazione tra Stati membri.

3. La presente direttiva completa il diritto comunitario relativo ai servizi della società dell'informazione facendo salvo il livello di tutela, in particolare, della sanità pubblica e dei consumatori, garantito dagli strumenti comunitari e dalla legislazione nazionale di attuazione nella misura in cui esso non limita la libertà di fornire servizi della società dell'informazione.

(...)

5. La presente direttiva non si applica:

(...)

b) alle questioni relative ai servizi della società dell'informazione oggetto delle direttive [95/46] e [97/66];

(...)».

10 L'articolo 2 della direttiva 2000/31 è così formulato:

«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 [del Parlamento europeo e del Consiglio, del 22 giugno 1998, che prevede una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche (GU 1998, L 204, pag. 37)], come modificata dalla direttiva 98/48/CE [del Parlamento europeo e del Consiglio, del 20 luglio 1998 (GU 1998, L 217, pag. 18)].

(...)».

11 L'articolo 15 della direttiva 2000/31 prevede quanto segue:

«1. Nella prestazione dei servizi di cui agli articoli 12, 13 e 14, gli Stati membri non impongono ai prestatori un obbligo generale di sorveglianza sulle informazioni che trasmettono o memorizzano né un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite.

2. Gli Stati membri possono stabilire che i prestatori di servizi della società dell'informazione siano tenuti ad informare senza indugio la pubblica autorità competente di presunte attività o informazioni illecite dei destinatari dei loro servizi o a comunicare alle autorità competenti, a loro richiesta, informazioni che consentano l'identificazione dei destinatari dei loro servizi con cui hanno accordi di memorizzazione dei dati».

Direttiva 2002/21

12 A termini del considerando 10 della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (direttiva quadro) (GU 2002, L 108, pag. 33):

«La definizione di "servizio della società dell'informazione" di cui all'articolo 1 della direttiva [98/34, come modificata dalla direttiva 98/48,] abbraccia una vasta gamma di attività economiche che si svolgono online. La maggior parte di tali attività non rientrano nel campo di applicazione della presente direttiva in quanto non consistono interamente o prevalentemente nella trasmissione di segnali su reti di comunicazione elettronica. La telefonia vocale e i servizi di posta elettronica sono disciplinati dalla presente direttiva. La stessa impresa, ad esempio un fornitore di servizi Internet, può offrire sia un servizio di comunicazione elettronica, quale l'accesso ad Internet, sia servizi non contemplati dalla presente direttiva, quali la fornitura di materiale in rete».

13 L'articolo 2 della direttiva 2002/21 prevede quanto segue:

«Ai fini della presente direttiva si intende per:

(...)

c) "servizio di comunicazione elettronica", i servizi forniti di norma a pagamento consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, ma ad esclusione dei servizi che forniscono contenuti trasmessi utilizzando reti e servizi di comunicazione elettronica o che esercitano un controllo editoriale su tali contenuti; sono inoltre esclusi i servizi della società dell'informazione di cui all'articolo 1 della direttiva [98/34] non consistenti interamente o prevalentemente nella trasmissione di segnali su reti di comunicazione elettronica;

(...)».

Direttiva 2002/58

14 I considerando 2, 6, 7, 11, 22, 26 e 30 della direttiva 2002/58 enunciano quanto segue:

«(2) La presente direttiva mira a rispettare i diritti fondamentali e si attiene ai principi riconosciuti in particolare dalla [Carta]. In particolare, la presente direttiva mira a garantire il pieno rispetto dei diritti di cui agli articoli 7 e 8 di tale Carta.

(...)

(6) L'Internet ha sconvolto le tradizionali strutture del mercato fornendo un'infrastruttura mondiale comune per la fornitura di un'ampia serie di servizi di comunicazione elettronica. I servizi di comunicazione elettronica accessibili al pubblico attraverso l'Internet aprono nuove possibilità agli utenti ma rappresentano anche nuovi pericoli per i loro dati personali e la loro vita privata.

(7) Nel settore delle reti pubbliche di comunicazione occorre adottare disposizioni legislative, regolamentari e tecniche specificamente finalizzate a tutelare i diritti e le libertà fondamentali delle persone fisiche e i legittimi interessi delle persone giuridiche, con particolare riferimento all'accresciuta capacità di memorizzazione e trattamento dei dati relativi agli abbonati e agli utenti.

(...)

(11) La presente direttiva, analogamente alla direttiva [95/46], non affronta le questioni relative alla tutela dei diritti e delle libertà fondamentali inerenti ad attività che non sono disciplinate dal diritto [dell'Unione]. 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, [firmata a Roma il 4 novembre 1950,] 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.

(...)

(22) Il divieto di memorizzare comunicazioni e i relativi dati sul traffico da parte di persone diverse dagli utenti o senza il loro consenso non è inteso a vietare eventuali memorizzazioni automatiche, intermedie e temporanee di tali informazioni fintanto che ciò viene fatto unicamente a scopo di trasmissione nella rete di comunicazione elettronica e a condizione che l'informazione non sia memorizzata per un periodo superiore a quanto necessario per la trasmissione e ai fini della gestione del traffico e che durante il periodo di memorizzazione sia assicurata la riservatezza dell'informazione. (...)

(...)

(26) I dati relativi agli abbonati sottoposti a trattamento nell'ambito di reti di comunicazione elettronica per stabilire i collegamenti e per trasmettere informazioni contengono informazioni sulla vita privata delle persone fisiche e riguardano il diritto al rispetto della loro corrispondenza o i legittimi interessi delle persone giuridiche. Tali dati possono essere memorizzati solo nella misura necessaria per la fornitura del servizio ai fini della fatturazione e del pagamento per l'interconnessione, nonché per un periodo di tempo limitato. Qualsiasi ulteriore trattamento di tali dati (...) può essere autorizzato soltanto se l'abbonato abbia espresso il proprio consenso in base ad informazioni esaurienti ed accurate date dal fornitore dei servizi di comunicazione elettronica accessibili al pubblico circa la natura dei successivi trattamenti che egli intende effettuare e circa il diritto dell'abbonato di non dare o di revocare il proprio consenso a tale trattamento. I dati relativi al traffico utilizzati per la commercializzazione dei servizi di comunicazione (...) dovrebbero inoltre essere cancellati o resi anonimi (…).

(...)

(30) I sistemi per la fornitura di reti e servizi di comunicazione elettronica dovrebbero essere progettati per limitare al minimo la quantità di dati personali necessari. (...)».

15 L'articolo 1 della direttiva 2002/58, intitolato «Finalità e campo d'applicazione», dispone quanto segue:

«1. La presente direttiva prevede l'armonizzazione delle disposizioni nazionali necessarie per assicurare un livello equivalente di tutela dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata e alla riservatezza, con riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche e per assicurare la libera circolazione di tali dati e delle apparecchiature e dei servizi di comunicazione elettronica all'interno [dell'Unione europea].

2. Ai fini di cui al paragrafo 1, le disposizioni della presente direttiva precisano e integrano la direttiva [95/46]. Esse prevedono inoltre la tutela dei legittimi interessi degli abbonati che sono persone giuridiche.

3. La presente direttiva non si applica alle attività che esulano dal campo di applicazione del [TFUE], 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».

16 L'articolo 2 della direttiva 2002/58, intitolato «Definizioni», così recita:

«Salvo diversa disposizione, ai fini della presente direttiva si applicano le definizioni di cui alla direttiva [95/46] e alla direttiva [2002/21].

Si applicano inoltre le seguenti definizioni:

a) "utente": qualsiasi persona fisica che utilizzi un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

b) "dati relativi al traffico": qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

c) "dati relativi all'ubicazione": ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indichi la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

d) "comunicazione": ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse, come parte di un servizio di radiodiffusione, al pubblico tramite una rete di comunicazione elettronica salvo quando le informazioni possono essere collegate all'abbonato o utente che riceve le informazioni che può essere identificato;

(...)».

17 L'articolo 3 della direttiva 2002/58, intitolato «Servizi interessati», prevede quanto segue:

«La presente direttiva si applica al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche nella Comunità, comprese le reti di comunicazione pubbliche che supportano i dispositivi di raccolta e di identificazione dei dati».

18 A termini dell'articolo 5 della direttiva 2002/58, intitolato «Riservatezza delle comunicazioni»:

«1. 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.

(...)

3. Gli Stati membri assicurano che l'archiviazione di informazioni oppure l'accesso a informazioni già archiviate nell'apparecchiatura terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente in questione abbia espresso preliminarmente il proprio consenso, dopo essere stato informato in modo chiaro e completo, a norma della direttiva [95/46], tra l'altro sugli scopi del trattamento. Ciò non vieta l'eventuale archiviazione tecnica o l'accesso al solo fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente a erogare tale servizio».

19 L'articolo 6 della direttiva 2002/58, intitolato «Dati sul traffico», dispone quanto segue:

«1. 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.

2. 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.

3. Ai fini della commercializzazione dei servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico ha facoltà di sottoporre a trattamento i dati di cui al paragrafo 1 nella misura e per la durata necessaria per siffatti servizi, o per la commercializzazione, sempre che l'abbonato o l'utente a cui i dati si riferiscono abbia espresso preliminarmente il proprio consenso. Gli abbonati o utenti hanno la possibilità di ritirare il loro consenso al trattamento dei dati relativi al traffico in qualsiasi momento.

(...)

5. Il trattamento dei dati relativi al traffico ai sensi dei paragrafi da 1 a 4 deve essere limitato alle persone che agiscono sotto l'autorità dei fornitori della rete pubblica di comunicazione elettronica e dei servizi di comunicazione elettronica accessibili al pubblico che si occupano della fatturazione o della gestione del traffico, delle indagini per conto dei clienti, dell'accertamento delle frodi, della commercializzazione dei servizi di comunicazione elettronica o della prestazione di servizi a valore aggiunto. Il trattamento deve essere limitato a quanto è strettamente necessario per lo svolgimento di tali attività».

20 L'articolo 9 di detta direttiva, intitolato «Dati relativi all'ubicazione diversi dai dati relativi al traffico», prevede, al paragrafo 1, quanto segue:

«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. (...)».

21 L'articolo 15 di tale direttiva, intitolato «Applicazione di alcune disposizioni della direttiva [95/46]», enuncia quanto segue:

«1. Gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva [95/46], una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica, e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l'altro adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo. Tutte le misure di cui al presente paragrafo sono conformi ai principi generali del diritto [dell'Unione], compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea.

(...)

2. Le disposizioni del capo III della direttiva [95/46] relative ai ricorsi giurisdizionali, alle responsabilità e alle sanzioni si applicano relativamente alle disposizioni nazionali adottate in base alla presente direttiva e con riguardo ai diritti individuali risultanti dalla stessa.

(...)».

Regolamento 2016/679

22 Il considerando 10 del regolamento 2016/679 enuncia quanto segue:

«Al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati dovrebbe essere equivalente in tutti gli Stati membri. È opportuno assicurare un'applicazione coerente e omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione. (...)».

23 L'articolo 2 di tale regolamento così dispone:

«1. Il presente regolamento si applica 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.

2. Il presente regolamento non si applica ai trattamenti di dati personali:

a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;

b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE;

(...)

d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

(...)

4. Il presente regolamento non pregiudica pertanto l'applicazione della direttiva [2000/31], in particolare le norme relative alla responsabilità dei prestatori intermediari di servizi di cui agli articoli da 12 a 15 della medesima direttiva».

24 L'articolo 4 di detto regolamento prevede quanto segue:

«Ai fini del presente regolamento s'intende per:

1) "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;

2) "trattamento" 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;

(...)».

25 L'articolo 5 del regolamento 2016/679 così dispone:

«1. I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza");

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali ("limitazione della finalità");

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati");

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("esattezza");

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato ("limitazione della conservazione");

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali ("integrità e riservatezza").

(...)».

26 L'articolo 6 di tale regolamento è così formulato:

«1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

(...)

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

(...)

3. La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita:

a) dal diritto dell'Unione; o

b) dal diritto dello Stato membro cui è soggetto il titolare del trattamento.

La finalità del trattamento è determinata in tale base giuridica (...). Tale base giuridica potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX. Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito.

(...)».

27 L'articolo 23 di detto regolamento prevede quanto segue:

«1. 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.

2. 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».

28 L'articolo 79, paragrafo 1, di detto regolamento così recita:

«Fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile, compreso il diritto di proporre reclamo a un'autorità di controllo ai sensi dell'articolo 77, ogni interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora ritenga che i diritti di cui gode a norma del presente regolamento siano stati violati a seguito di un trattamento».

29 A termini dell'articolo 94 del regolamento 2016/679:

«1. La direttiva [95/46] è abrogata a decorrere dal 25 maggio 2018.

2. I riferimenti alla direttiva abrogata si intendono fatti al presente regolamento. I riferimenti al gruppo per la tutela delle persone con riguardo al trattamento dei dati personali istituito dall'articolo 29 della direttiva [95/46] si intendono fatti al comitato europeo per la protezione dei dati istituito dal presente regolamento».

30 L'articolo 95 del suddetto regolamento dispone quanto segue:

«Il presente regolamento non impone obblighi supplementari alle persone fisiche o giuridiche in relazione al trattamento nel quadro della fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nell'Unione, per quanto riguarda le materie per le quali sono soggette a obblighi specifici aventi lo stesso obiettivo fissati dalla direttiva [2002/58]».

Diritto francese

Codice della sicurezza interna

31 Il libro VIII della parte legislativa del code de la sécurité intérieure (codice della sicurezza interna; in prosieguo: il «CSI») contiene, agli articoli da L. 801-1 a L. 898-1, norme relative all'intelligence.

32 L'articolo L. 811-3 del CSI così dispone:

«Esclusivamente al fine dell'esercizio delle rispettive funzioni, i servizi di informazione specializzati possono avvalersi delle tecniche di cui al titolo V del presente libro per la raccolta delle informazioni relative alla difesa e alla promozione dei seguenti interessi fondamentali della Nazione:

1° l'indipendenza nazionale, l'integrità del territorio e la difesa nazionale;

2° gli interessi superiori della politica estera, l'esecuzione degli impegni europei e internazionali della Francia e la prevenzione di qualsiasi forma di ingerenza straniera;

3° gli interessi superiori economici, industriali e scientifici della Francia;

4° la prevenzione del terrorismo;

5° la prevenzione:
   a) degli attentati alla forma repubblicana delle istituzioni;
   b) delle azioni dirette al mantenimento o alla ricostituzione di gruppi sciolti in applicazione dell'articolo L. 212-1;
   c) delle violenze collettive tali da compromettere gravemente il mantenimento della legge e dell'ordine;

6° la prevenzione della criminalità e della delinquenza organizzate;

7° la prevenzione della proliferazione delle armi di distruzione di massa».

33 L'articolo L. 811-4 del CSI enuncia quanto segue:

«Un decreto adottato del Conseil d'État [Consiglio di Stato], previo parere della Commission nationale de contrôle des techniques de renseignement [Commissione nazionale di controllo delle tecniche di informazione, Francia], designa i servizi, diversi dai servizi di informazione specializzati, dipendenti dai Ministri della Difesa, dell'Interno e della Giustizia, nonché dai ministri incaricati dell'economia, del bilancio e delle dogane, che possono essere autorizzati a ricorrere alle tecniche di cui al titolo V del presente libro alle condizioni previste nel medesimo libro. Esso precisa, per ciascun servizio, le finalità di cui all'articolo L. 811-3 e le tecniche che possono dare luogo ad autorizzazione».

34 L'articolo L. 821-1, primo comma, del CSI precisa quanto segue:

«L'attuazione sul territorio nazionale delle tecniche di raccolta di informazioni di cui ai capi da I a IV del titolo V del presente libro è soggetta alla preventiva autorizzazione del Primo ministro, rilasciata previo parere della Commissione nazionale di controllo delle tecniche di informazione».

35 L'articolo L. 821-2 del CSI prevede quanto segue:

«L'autorizzazione di cui all'articolo L. 821-1 è rilasciata su richiesta scritta e motivata del Ministro della Difesa, del Ministro dell'Interno, del Ministro della Giustizia o dei ministri incaricati dell'economia, del bilancio o delle dogane. Ogni ministro può delegare tale potere individualmente solo a collaboratori diretti ammessi al segreto della difesa nazionale.

La richiesta indica:

1° la tecnica o le tecniche da attuare;

2° il servizio per il quale è presentata la richiesta;

3° la o le finalità perseguite;

4° il motivo o i motivi delle misure;

5° la durata di validità dell'autorizzazione;

6° la persona o le persone, il luogo o i luoghi ovvero i veicoli interessati.

Ai fini dell'applicazione del punto 6°, le persone la cui identità è ignota possono essere designate mediante i loro identificativi o il loro status e i luoghi o veicoli possono essere designati con riferimento alle persone oggetto della domanda.

(…)».

36 Ai sensi dell'articolo L. 821-3, primo comma, del CSI:

«La richiesta è comunicata al presidente o, in mancanza, a uno dei membri della Commissione nazionale di controllo delle tecniche di informazione tra quelli menzionati ai punti 2° e 3° dell'articolo L. 831-1, il quale trasmette un parere al Primo ministro entro ventiquattro ore. Se la richiesta è esaminata dalla formazione ristretta o dalla formazione plenaria della Commissione, il Primo ministro ne viene informato senza ritardo e il parere è emesso entro settantadue ore».

37 L'articolo L. 821-4 del CSI dispone quanto segue:

«L'autorizzazione all'attuazione delle tecniche di cui ai capi da I a IV del titolo V del presente libro è rilasciata dal Primo ministro per una durata massima di quattro mesi. (…) L'autorizzazione contiene le motivazioni e le menzioni previste ai punti dal 1° al 6° dell'articolo L. 821-2. Tutte le autorizzazioni sono rinnovabili alle stesse condizioni previste nel presente capo.

Se è rilasciata dopo un parere negativo della Commissione nazionale di controllo delle tecniche di informazione, l'autorizzazione indica i motivi per i quali tale parere non è stato accolto.

(...)».

38 L'articolo L. 833-4 del CSI, contenuto nel capo III del suddetto titolo, dispone quanto segue:

«La Commissione, di propria iniziativa o su reclamo di chiunque intenda verificare che nessuna tecnica di informazione sia attuata irregolarmente nei suoi confronti, procede al controllo della o delle tecniche di cui trattasi al fine di verificare che siano state o siano attuate nel rispetto del presente libro. Essa informa il reclamante di avere svolto le necessarie verifiche, senza confermare o negare la loro attuazione».

39 L'articolo L. 841-1, primo e secondo comma, del CSI è così formulato:

«Fatte salve le disposizioni particolari di cui all'articolo L. 854-9 del presente codice, il Conseil d'État [Consiglio di Stato] è competente a conoscere, alle condizioni previste nel libro VII, titolo VII, capo III bis, del code de justice administrative [codice della giustizia amministrativa], dei ricorsi concernenti l'attuazione delle tecniche di informazione di cui al titolo V del presente libro.

Esso può essere adito da:

1° chiunque intenda verificare che nessuna tecnica di informazione sia attuata in maniera irregolare nei suoi confronti e dimostri che è stata previamente espletata la procedura di cui all'articolo L. 833-4;

2° la Commissione nazionale di controllo delle tecniche di informazione, alle condizioni previste dall'articolo L. 833-8».

40 Il titolo V del libro VIII della parte legislativa del CSI, relativo alle «tecniche di raccolta di informazioni soggette ad autorizzazione», contiene, in particolare, un capo I, intitolato «Accesso amministrativo ai dati di connessione», che comprende gli articoli da L. 851-1 a L. 851-7 del CSI.

41 L'articolo L. 851-1 del CSI così dispone:

«In conformità alle condizioni previste nel capo I del titolo II del presente libro, può essere autorizzata la raccolta, in capo agli operatori del settore delle comunicazioni elettroniche, ai soggetti indicati all'articolo L. 34-1 del [CPCE] e a quelli menzionati al paragrafo I, punti 1 e 2, dell'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] [(JORF del 22 giugno 2004, pag. 11168)], delle informazioni o dei documenti trattati o conservati attraverso le loro reti o servizi di comunicazione elettronica, ivi compresi i dati tecnici relativi all'identificazione dei numeri di abbonamento o di connessione ai servizi di comunicazione elettronica, al censimento di tutti i numeri di abbonamento o di connessione di una determinata persona, all'ubicazione delle apparecchiature terminali utilizzate nonché alle comunicazioni di un abbonato concernenti l'elenco dei numeri chiamati e chiamanti, la durata e la data delle comunicazioni.

In deroga all'articolo L. 821-2, le richieste scritte e motivate riguardanti i dati tecnici relativi all'identificazione dei numeri di abbonamento o di connessione a servizi di comunicazione elettronica o al censimento di tutti i numeri di abbonamento o di connessione di una determinata persona sono trasmesse direttamente alla Commissione nazionale di controllo delle tecniche di informazione dagli agenti individualmente designati e autorizzati dei servizi di informazione di cui agli articoli L. 811-2 e L. 811-4. La Commissione emette il proprio parere alle condizioni previste dall'articolo L. 821-3.

Un servizio del Primo ministro è incaricato di raccogliere le informazioni o i documenti presso gli operatori e i soggetti di cui al primo comma del presente articolo. La Commissione nazionale di controllo delle tecniche di informazione dispone di un accesso permanente, completo, diretto e immediato alle informazioni o ai documenti raccolti.

Le modalità di applicazione del presente articolo sono stabilite con decreto del Conseil d'État [Consiglio di Stato], adottato previo parere della Commission nationale de l'informatique et des libertés [Commissione nazionale per l'informatica e le libertà, Francia] e della Commission nationale de contrôle des techniques de renseignement [Commissione nazionale di controllo delle tecniche di informazione, Francia]».

42 L'articolo L. 851-2 del CSI enuncia quanto segue:

«I. – 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.

I°bis. 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.

(...)».

43 L'articolo L. 851-3 del CSI prevede quanto segue:

«I. – 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.

II. – La Commissione nazionale di controllo delle tecniche di informazione emette un parere sulla richiesta di autorizzazione relativa ai trattamenti automatizzati e sui parametri di rilevazione adottati. Essa dispone di un accesso permanente, completo e diretto a tali trattamenti nonché alle informazioni e ai dati raccolti. Essa è informata di ogni modifica apportata ai trattamenti e ai parametri e può formulare raccomandazioni.

La prima autorizzazione all'attuazione dei trattamenti automatizzati prevista al paragrafo I del presente articolo è rilasciata per un periodo di due mesi. L'autorizzazione può essere rinnovata alle condizioni relative alla durata previste al capo I del titolo II del presente libro. La richiesta di rinnovo contiene l'indicazione del numero di identificativi segnalati dal trattamento automatizzato e un'analisi della pertinenza di tali segnalazioni.

III. – Le condizioni previste all'articolo L. 871-6 sono applicabili alle operazioni materiali effettuate per tale attuazione dagli operatori e dai soggetti di cui all'articolo L.851-1.

IV. – Qualora i trattamenti menzionati al paragrafo I del presente articolo rilevino dati che possono qualificare l'esistenza di una minaccia di natura terroristica, il Primo ministro o uno dei soggetti da questo delegati può autorizzare, previo parere della Commissione nazionale di controllo delle tecniche di informazione emesso alle condizioni previste al capo I del titolo II del presente libro, l'identificazione della persona o delle persone interessate e la raccolta dei relativi dati. Tali dati sono utilizzati entro sessanta giorni a decorrere dalla raccolta e sono distrutti alla scadenza di detto termine, salvo che sussistano elementi seri che confermino l'esistenza di una minaccia terroristica collegata a una o più persone interessate.

(...)».

44 L'articolo L. 851-4 del CSI è così formulato:

«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».

45 L'articolo R. 851-5 del CSI, contenuto nella parte regolamentare di tale codice, prevede quanto segue:

«I. – Le informazioni o i documenti di cui all'articolo L. 851-1, ad eccezione del contenuto della corrispondenza intercorsa o delle informazioni consultate, sono:

1° quelli elencati agli articoli R. 10-13 e R. 10-14 del [CPCE] e all'articolo 1 del decreto [n. 2011-219];

2° i dati tecnici diversi da quelli menzionati al punto 1°:

a) che consentono di localizzare le apparecchiature terminali;

b) relativi all'accesso delle apparecchiature terminali alle reti o ai servizi di comunicazione al pubblico online;

c) relativi alla trasmissione delle comunicazioni elettroniche attraverso le reti;

d) relativi all'identificazione e all'autenticazione di un utente, di una connessione, di una rete o di un servizio di comunicazione al pubblico online;

e) relativi alle caratteristiche delle apparecchiature terminali e ai dati di configurazione dei rispettivi software.

II. – Possono raccogliersi in applicazione dell'articolo L. 851-1 esclusivamente le informazioni e i documenti menzionati al punto 1° del paragrafo I. Tale raccolta ha luogo in tempo differito.

Fatta salva l'applicazione dell'articolo R. 851-9, le informazioni elencate al punto 2° del paragrafo I possono essere raccolte solo in applicazione degli articoli L. 851-2 e L. 851-3 alle condizioni e nei limiti previsti da tali articoli».

CPCE

46 L'articolo L. 34-1 del CPCE dispone quanto segue:

«I. – Il presente articolo si applica al trattamento dei dati personali nella prestazione al pubblico di servizi di comunicazione elettronica; in particolare, si applica alle reti che supportano i dispositivi di raccolta e di identificazione dei dati.

II. – Gli operatori di comunicazione elettronica, e in particolare le persone la cui attività consiste nell'offrire accesso a servizi di comunicazione al pubblico online, eliminano o rendono anonimi tutti i dati relativi al traffico, fatte salve le disposizioni dei paragrafi III, IV, V e VI.

Le persone che forniscono al pubblico servizi di comunicazione elettronica stabiliscono, nel rispetto delle disposizioni del comma precedente, procedure interne che consentano di soddisfare le richieste delle autorità competenti.

Le persone che, nell'esercizio di un'attività professionale principale o accessoria, offrono al pubblico una connessione che consente la comunicazione online tramite accesso alla rete, anche a titolo gratuito, sono tenute al rispetto delle disposizioni applicabili agli operatori di comunicazione elettronica ai sensi del presente articolo.

III. – Ai fini dell'indagine, dell'accertamento e del perseguimento dei reati o dell'inadempimento dell'obbligo definito all'articolo L. 336-3 del code de la propriété intellectuelle [codice della proprietà intellettuale] o ai fini della prevenzione di attacchi ai sistemi di trattamento automatizzato dei dati previsti e puniti dagli articoli da 323-1 a 323-3-1 del code pénal [codice penale], e al solo scopo di consentire, ove necessario, la messa a disposizione dell'autorità giudiziaria o dell'alta autorità di cui all'articolo L. 331-12 del codice della proprietà intellettuale o dell'autorità nazionale per la sicurezza dei sistemi di informazione menzionata all'articolo L. 2321-1 del code de la défense [codice della difesa], possono essere rinviate per un periodo massimo di un anno le operazioni dirette ad eliminare o a rendere anonime determinate categorie di dati tecnici. Con decreto adottato dopo aver consultato il Conseil d'État [Consiglio di Stato], e previo parere della Commissione nazionale per l'informatica e le libertà, sono stabilite, entro i limiti fissati al paragrafo VI, le suddette categorie di dati e la durata della loro conservazione, in funzione dell'attività degli operatori e della natura delle comunicazioni, nonché, se del caso, le modalità di compensazione delle spese identificabili e specifiche delle prestazioni garantite a tale titolo, su richiesta dello Stato, dagli operatori.

(...)

VI. – I dati conservati e trattati alle condizioni di cui ai paragrafi III, IV e V riguardano esclusivamente l'identificazione degli utenti dei servizi prestati dagli operatori, le caratteristiche tecniche delle comunicazioni fornite da questi ultimi e l'ubicazione delle apparecchiature terminali.

Essi non possono riguardare in alcun caso il contenuto della corrispondenza intercorsa o delle informazioni consultate, in qualsiasi modo, nell'ambito di tali comunicazioni.

La conservazione e il trattamento dei dati sono effettuati nel rispetto delle disposizioni della loi n. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [legge n. 78-17 del 6 gennaio 1978, relativa all'informatica, ai file e alle libertà].

Gli operatori adottano le misure necessarie per impedire l'utilizzo di tali dati a fini diversi da quelli previsti nel presente articolo».

47 L'articolo R. 10-13 del CPCE è così formulato:

«I. – 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.

II. – 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.

III. – I dati di cui al presente articolo sono conservati per un periodo di un anno a decorrere dalla data della loro registrazione.

IV. – 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 [codice di procedura penale]».

48 L'articolo R. 10-14 del CPCE prevede quanto segue:

«I. – In applicazione dell'articolo L. 34-1, paragrafo IV, gli operatori di comunicazioni elettroniche sono autorizzati a conservare, ai fini delle loro operazioni di fatturazione e di pagamento, i dati tecnici che consentono di identificare l'utente nonché i dati menzionati all'articolo R. 10-13, paragrafo I, lettere b), c) e d).

II. – Per le attività di telefonia gli operatori possono conservare, oltre ai dati menzionati al paragrafo I, i dati tecnici relativi all'ubicazione della comunicazione, all'identificazione del destinatario o dei destinatari della comunicazione e i dati che consentono la fatturazione.

III. – I dati di cui ai paragrafi I e II del presente articolo possono essere conservati solo se sono necessari ai fini della fatturazione e del pagamento dei servizi resi. La loro conservazione deve essere limitata al tempo strettamente necessario a tale finalità e non può avere una durata superiore a un anno.

IV. – Per la sicurezza delle reti e degli impianti, gli operatori possono conservare per un periodo non superiore a tre mesi:

a) i dati che consentono di identificare l'origine della comunicazione;

b) le caratteristiche tecniche nonché la data, l'ora e la durata di ogni comunicazione;

c) i dati tecnici che consentono di identificare il destinatario o i destinatari della comunicazione;

d) i dati relativi ai servizi complementari richiesti o utilizzati e i loro fornitori».

Legge n. 2004-575, del 21 giugno 2004, per la fiducia nell'economia digitale

49 L'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) (JORF del 22 giugno 2004, pag. 11168; in prosieguo: la «LCEN»), prevede quanto segue:

«I. – 1. Le persone la cui attività consiste nell'offrire al pubblico un accesso a servizi di comunicazione online informano i loro abbonati dell'esistenza di mezzi tecnici che consentono di limitare l'accesso a determinati servizi o di selezionarli e propongono loro almeno uno di tali mezzi.

(...)

2. Le persone fisiche o giuridiche che garantiscono, anche a titolo gratuito, mediante la messa a disposizione del pubblico tramite servizi di comunicazione al pubblico online, l'archiviazione di segnali, scritti, immagini, suoni o messaggi di qualsiasi natura forniti dai destinatari di detti servizi non sono civilmente responsabili per le attività o le informazioni memorizzate su richiesta di un destinatario di tali servizi se non erano effettivamente a conoscenza del loro carattere illecito o di fatti e circostanze da cui risulta tale illiceità o se, a partire dal momento in cui ne hanno avuto conoscenza, hanno agito tempestivamente per ritirare tali dati o renderli inaccessibili.

(...)

II. – 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.

Esse forniscono alle persone che pubblicano un servizio di comunicazione al pubblico online mezzi tecnici che consentano loro di soddisfare le condizioni di identificazione previste al paragrafo III.

L'autorità giudiziaria può chiedere ai prestatori di cui al paragrafo I, punti 1 e 2, che le siano comunicati i dati indicati nel primo comma.

Al trattamento di tali dati si applicano le disposizioni degli articoli 226-17, 226-21 e 226-22 del codice penale.

Un decreto del Conseil d'État [Consiglio di Stato], adottato previo parere della Commissione nazionale per l'informatica e le libertà, definisce i dati menzionati nel primo comma nonché la durata e le modalità della loro conservazione.

(...)».

Decreto n. 2011-219

50 Il capo I del decreto n. 2011-219, adottato sul fondamento dell'articolo 6, paragrafo II, ultimo comma, della LCEN, contiene gli articoli da 1 a 4 di detto decreto.

51 L'articolo 1 del decreto n. 2011-219 così dispone:

«I dati di cui all'articolo 6, paragrafo II, della [LCEN], che le persone interessate sono tenute a conservare in forza di tale disposizione, sono i seguenti:

1° per le persone menzionate al paragrafo I, punto 1, del medesimo articolo e per ciascuna connessione di loro abbonati:

a) l'identificativo della connessione;

b) l'identificativo attribuito da tali persone all'abbonato;

c) l'identificativo del terminale utilizzato per la connessione ove vi abbiano accesso;

d) i dati nonché l'ora di inizio e di fine della connessione;

e) le caratteristiche della linea dell'abbonato;

2° per le persone menzionate al paragrafo I, punto 2, del medesimo articolo e per ciascuna operazione di creazione:

a) l'identificativo della connessione all'origine della comunicazione;

b) l'identificativo attribuito dal sistema di informazione al contenuto oggetto dell'operazione;

c) i tipi di protocolli utilizzati per la connessione al servizio e per il trasferimento dei contenuti;

d) la natura dell'operazione;

e) la data e l'ora dell'operazione;

f) l'identificativo utilizzato dall'autore dell'operazione, ove l'abbia fornito;

3° per le persone menzionate al paragrafo I, punti 1 e 2, del medesimo articolo, le informazioni fornite da un utente al momento della sottoscrizione di un contratto o della creazione di un account:

a) l'identificativo di tale connessione al momento della creazione dell'account;

b) il nome e cognome o la ragione sociale;

c) gli indirizzi postali associati;

d) gli pseudonimi utilizzati;

e) gli indirizzi di posta elettronica o di account associati;

f) i numeri di telefono;

g) la password nonché i dati che consentono di verificarla o modificarla, nella loro ultima versione aggiornata;

4° per le persone menzionate al paragrafo I, punti 1 e 2, del medesimo articolo, qualora la sottoscrizione del contratto o dell'account sia a pagamento, le seguenti informazioni relative al pagamento, per ciascuna operazione di pagamento:

a) il tipo di pagamento utilizzato;

b) il riferimento del pagamento;

c) l'importo;

d) la data e l'ora dell'operazione.

I dati di cui ai punti 3° e 4° devono essere conservati solo nella misura in cui le persone interessate li raccolgono abitualmente».

52 L'articolo 2 di tale decreto è così formulato:

«Il contributo alla creazione di contenuto comprende le operazioni relative a:

a) creazioni iniziali di contenuti;

b) modifiche dei contenuti e di dati connessi ai contenuti;

c) cancellazioni di contenuti».

53 L'articolo 3 di detto decreto prevede quanto segue:

«I dati di cui all'articolo 1 sono conservati per un periodo di un anno:

a) per i dati di cui ai punti 1° e 2°, a decorrere dalla data della creazione dei contenuti, per ciascuna operazione che contribuisce alla creazione di un contenuto come definita all'articolo 2;

b) per i dati di cui al punto 3°, a decorrere dalla data della risoluzione del contratto o dalla chiusura dell'account;

c) per i dati di cui al punto 4°, a decorrere dalla data di emissione della fattura o dell'operazione di pagamento, per ciascuna fattura o operazione di pagamento».

Diritto belga

54 La legge del 29 maggio 2016 ha modificato, in particolare, la loi du 13 juin 2005 relative aux communications électroniques (legge del 13 giugno 2005 sulle comunicazioni elettroniche) (*Moniteur belge* del 20 giugno 2005, pag. 28070) (in prosieguo: la «legge del 13 giugno 2005»), il code d'instruction criminelle (codice di procedura penale) e la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (legge organica del 30 novembre 1998 sui servizi di intelligence e di sicurezza) (*Moniteur belge* del 18 dicembre 1998, pag. 40312; in prosieguo: la «legge del 30 novembre 1998»).

55 L'articolo 126 della legge del 13 giugno 2005, nella versione risultante dalla legge del 29 maggio 2016, così dispone:

«§ 1. Fatta salva la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel [legge dell'8 dicembre 1992 sulla protezione della vita privata in materia di trattamento dei dati personali], i fornitori di servizi di telefonia pubblica, compresi quelli via Internet, di accesso a Internet e di posta elettronica su Internet, gli operatori che forniscono reti pubbliche di comunicazioni elettroniche, nonché gli operatori che forniscono uno di tali servizi, conservano i dati di cui al paragrafo 3 che sono da essi generati o trattati nell'ambito della fornitura dei rispettivi servizi di comunicazione.

Il contenuto delle comunicazioni non è disciplinato dal presente articolo.

L'obbligo di conservare i dati di cui al paragrafo 3 si applica anche alle chiamate non completate, nella misura in cui tali dati siano, nell'ambito della fornitura dei servizi di comunicazione interessati:

1° per quanto riguarda i dati di telefonia, generati o trattati dagli operatori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione elettronica, oppure

2° per quanto riguarda i dati Internet, registrati da tali fornitori.

§ 2. Solamente le seguenti autorità possono ottenere, su semplice richiesta, dai fornitori e dagli operatori di cui al paragrafo 1, primo comma, dati conservati ai sensi del presente articolo, per le finalità e alle condizioni elencate in appresso:

1° le autorità giudiziarie, nell'ambito della ricerca, dell'accertamento e del perseguimento di reati, per l'esecuzione delle misure di cui agli articoli 46 bis e 88 bis del codice di procedura penale e nel rispetto delle condizioni previste da tali disposizioni;

2° i servizi di intelligence e di sicurezza, per la realizzazione di missioni di informazione che prevedono l'impiego dei metodi di raccolta di dati di cui agli articoli 16/2, 18/7 e 18/8 della loi du 30 novembre 1998 organique des services de renseignement et de sécurité [legge organica del 30 novembre 1998 sui servizi di intelligence e di sicurezza] e nel rispetto delle condizioni stabilite da detta legge;

3° gli ufficiali di polizia giudiziaria dell'[Institut belge des services postaux et des télécommunications (Istituto belga dei servizi postali e delle telecomunicazioni, Belgio)], nell'ambito della ricerca, dell'accertamento e del perseguimento di reati che costituiscono una violazione degli articoli 114 e 124 e del presente articolo;

4° i servizi di emergenza che prestano assistenza in loco, quando, in seguito a una chiamata d'emergenza, non ottengono dal fornitore o dall'operatore interessato i dati identificativi del chiamante con l'ausilio della banca dati di cui all'articolo 107, § 2, terzo comma, oppure ottengono dati incompleti o inesatti. Possono richiedersi solamente i dati identificativi del chiamante e non oltre le 24 ore successive alla chiamata;

5° l'ufficiale di polizia giudiziaria della Cellule des personnes disparues de la Police Fédérale [Cellula "persone scomparse" della Polizia federale, Belgio], nell'ambito delle proprie funzioni di soccorso a persone in stato di pericolo, di ricerca di persone la cui scomparsa desti sospetti e in presenza di circostanze o indizi gravi che indichino che l'integrità fisica della persona scomparsa è in pericolo imminente. Solamente i dati di cui al paragrafo 3, primo e secondo comma, riguardanti la persona scomparsa e conservati nel corso delle 48 ore che precedono la richiesta dei dati possono essere richiesti all'operatore o al fornitore interessato per mezzo di un'autorità di polizia designata dal Re;

6° il Service de médiation pour les télécommunications [Servizio di mediazione per le telecomunicazioni, Belgio], al fine di identificare la persona che abbia fatto un uso illecito di una rete o di un servizio di comunicazione elettronica, conformemente alle condizioni di cui all'articolo 43 bis, paragrafo 3, punto 7°, della loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques [legge del 21 marzo 1991 relativa alla riforma di alcune imprese pubbliche economiche]. Possono richiedersi solamente i dati identificativi.

I fornitori e gli operatori di cui al paragrafo 1, primo comma, assicurano che i dati di cui al paragrafo 3 siano accessibili senza alcuna limitazione a partire dal Belgio e che tali dati e qualsiasi altra informazione necessaria che riguardi detti dati siano trasmessi senza indugio ed esclusivamente alle autorità di cui al presente paragrafo.

Fatte salve altre disposizioni di legge, i fornitori e gli operatori di cui al paragrafo 1, primo comma, non possono utilizzare i dati conservati ai sensi del paragrafo 3 per altre finalità.

§ 3. I dati che consentono l'identificazione dell'utente o dell'abbonato e dei mezzi di comunicazione, ad eccezione dei dati previsti in particolare dai commi secondo e terzo, sono conservati per dodici mesi a decorrere dalla data a partire dalla quale è possibile effettuare per l'ultima volta una comunicazione tramite il servizio utilizzato.

I dati relativi all'accesso e alla connessione dell'apparecchiatura terminale alla rete e al servizio, nonché i dati relativi all'ubicazione di tale apparecchiatura, compreso il punto del terminale della rete, sono conservati per dodici mesi a decorrere dalla data della comunicazione.

I dati delle comunicazioni, ad eccezione del loro contenuto, comprese la loro origine e destinazione, sono conservati per dodici mesi a partire dalla data della comunicazione.

Il Re stabilisce, con decreto del Conseil de ministres [Consiglio dei ministri, Belgio], su proposta del Ministre de la Justice [Ministro della Giustizia, Belgio] e del Ministre [competente per le materie relative alle comunicazioni elettroniche] e previo parere della Commission de la protection de la vie privée [Commissione per la protezione della vita privata, Belgio] e dell'Istituto, i dati che devono essere conservati per ciascuna delle categorie di cui ai commi dal primo al terzo, nonché i requisiti che tali dati devono osservare.

(...)».

Procedimenti principali e questioni pregiudiziali

Causa C-511/18

56 Mediante atti introduttivi presentati il 30 novembre 2015 e il 16 marzo 2016, riuniti nel procedimento principale, la Quadrature du Net, la French Data Network, la Fédération des fournisseurs d'accès à Internet associatifs e la Igwan.net hanno adito il Conseil d'État (Consiglio di Stato, Francia) con ricorsi diretti all'annullamento dei decreti nn. 2015-1185, 2015-1211, 2015-1639 e 2016-67, lamentando, tra l'altro, che essi violerebbero la Costituzione francese, la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (in prosieguo: la «CEDU») nonché le direttive 2000/31 e 2002/58, lette alla luce degli articoli 7, 8 e 47 della Carta.

57 Per quanto riguarda, in particolare, i motivi vertenti sulla violazione della direttiva 2000/31, il giudice del rinvio rileva che le disposizioni dell'articolo L. 851-3 del CSI impongono agli operatori di comunicazione elettronica e ai prestatori di servizi tecnici «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». Questa tecnica sarebbe destinata unicamente a raccogliere, per un periodo limitato, tra tutti i dati di connessione trattati da tali operatori e prestatori, quelli che potrebbero presentare un legame con un siffatto grave reato. In tali circostanze, le disposizioni di cui trattasi, che non imporrebbero un obbligo generale di sorveglianza attiva, non violerebbero l'articolo 15 della direttiva 2000/31.

58 Per quanto riguarda i motivi vertenti sulla violazione della direttiva 2002/58, il giudice del rinvio considera che risulta in particolare dalle disposizioni di detta direttiva nonché dalla sentenza del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15; in prosieguo: la «sentenza Tele2», EU:C:2016:970), che le disposizioni nazionali che impongono obblighi ai fornitori di servizi di comunicazione elettronica, quali la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione di loro utenti e abbonati, ai fini indicati all'articolo 15, paragrafo 1, della direttiva citata, tra i quali figurano la salvaguardia della sicurezza nazionale, della difesa e della sicurezza pubblica, rientrano nell'ambito di applicazione della medesima direttiva nella misura in cui tali normative disciplinano l'attività dei suddetti fornitori. Lo stesso varrebbe per le normative che disciplinano l'accesso delle autorità nazionali ai dati nonché il loro utilizzo.

59 Il giudice del rinvio ne deduce che rientrano nell'ambito di applicazione della direttiva 2002/58 sia l'obbligo di conservazione risultante dall'articolo L. 851-1 del CSI sia gli accessi amministrativi ai suddetti dati, compresi quelli in tempo reale, previsti agli articoli L. 851-1, L. 851-2 e L. 851-4 di tale codice. Lo stesso vale, secondo detto giudice, per le disposizioni dell'articolo L. 851-3 del medesimo codice che, pur non prevedendo a carico degli operatori interessati un obbligo generale di conservazione, tuttavia impongono loro di attuare sulle proprie reti trattamenti automatizzati intesi a identificare collegamenti idonei a rivelare una minaccia terroristica.

60 Per contro, tale giudice ritiene che non rientrino nell'ambito di applicazione della direttiva 2002/58 le disposizioni del CSI oggetto delle domande di annullamento che riguardano le tecniche di raccolta di informazioni attuate direttamente dallo Stato, senza disciplinare le attività dei fornitori di servizi di comunicazione elettronica imponendo loro obblighi specifici. Dette disposizioni non potrebbero quindi essere considerate come attuative del diritto dell'Unione europea e, di conseguenza, i motivi vertenti sulla violazione, da parte delle stesse, della direttiva 2002/58 non potrebbero essere validamente invocati.

61 Pertanto, ai fini della definizione delle controversie vertenti sulla legittimità dei decreti nn. 2015-1185, 2015-1211, 2015-1639 e 2016-67 alla luce della direttiva 2002/58 in quanto adottati per l'attuazione degli articoli da L. 851-1 a L. 851-4 del CSI, si pongono tre questioni di interpretazione del diritto dell'Unione.

62 Per quel che riguarda l'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58, il giudice del rinvio si chiede, in primo luogo, se un obbligo di conservazione generalizzata e indifferenziata imposto ai fornitori di servizi di comunicazione elettronica sul fondamento degli articoli L. 851-1 e R. 851-5 del CSI non debba essere considerato, tenuto conto in particolare delle salvaguardie e dei controlli che accompagnano gli accessi amministrativi ai dati di connessione e il loro utilizzo, come un'ingerenza giustificata dal diritto alla sicurezza garantito dall'articolo 6 della Carta e dalle esigenze di sicurezza nazionale, la cui responsabilità è rimessa, a norma dell'articolo 4 TUE, unicamente agli Stati membri.

63 Per quanto concerne, in secondo luogo, gli altri obblighi che possono essere imposti ai fornitori di servizi di comunicazione elettronica, il giudice del rinvio rileva che le disposizioni dell'articolo L. 851-2 del CSI autorizzano, esclusivamente al fine della prevenzione del terrorismo, la raccolta delle informazioni o dei documenti previsti all'articolo L. 851-1 di detto codice, in capo agli stessi soggetti. Tale raccolta, che riguarderebbe unicamente una o più persone precedentemente identificate come potenzialmente collegate a una minaccia terroristica, sarebbe effettuata in tempo reale. Lo stesso varrebbe per le disposizioni dell'articolo L. 851-4 del suddetto codice che autorizzano la trasmissione

in tempo reale, da parte degli operatori, dei soli dati tecnici concernenti l'ubicazione delle apparecchiature terminali. Tali tecniche si applicherebbero per scopi e con modalità diverse dagli accessi amministrativi in tempo reale ai dati conservati ai sensi del CPCE e della LCEN, senza tuttavia porre a carico dei fornitori interessati un obbligo di conservazione aggiuntivo rispetto a quanto necessario ai fini della fatturazione e della fornitura dei loro servizi. Sulla stessa linea, le disposizioni dell'articolo L. 851-3 del CSI, che prevedono l'obbligo dei fornitori di servizi di attuare sulle loro reti un'analisi automatizzata delle connessioni, non implicherebbero nemmeno una conservazione generalizzata e indifferenziata.

64 Orbene, da un lato, il giudice del rinvio considera che sia la conservazione generalizzata e indifferenziata sia l'accesso in tempo reale ai dati di connessione presentano, in un contesto segnato da gravi e persistenti minacce alla sicurezza nazionale, relative in particolare al rischio di terrorismo, un'utilità dal punto di vista operativo senza equivalenti. Infatti, la conservazione generalizzata e indifferenziata consentirebbe ai servizi di informazione di accedere ai dati relativi alle comunicazioni prima che siano individuati i motivi che inducono a ritenere che l'interessato integri una minaccia per la sicurezza pubblica, la difesa o la sicurezza dello Stato. Inoltre, gli accessi in tempo reale ai dati di connessione permetterebbero di monitorare, con un elevato grado di reattività, i comportamenti di individui che possono rappresentare una minaccia attuale per l'ordine pubblico.

65 Dall'altro, la tecnica prevista all'articolo L. 851-3 del CSI consentirebbe di individuare, sulla base di criteri all'uopo precisamente definiti, i soggetti il cui comportamento, alla luce in particolare delle loro modalità di comunicazione, può rivelare una minaccia terroristica.

66 In terzo luogo, per quanto riguarda l'accesso delle autorità competenti ai dati conservati, il giudice del rinvio si chiede se la direttiva 2002/58, letta alla luce della Carta, debba essere interpretata nel senso che essa subordina sempre la regolarità delle procedure di raccolta dei dati di connessione a un obbligo di informazione degli interessati, ove tale informazione non sia più suscettibile di compromettere le indagini condotte dalle autorità competenti, o se tali procedure possano essere considerate regolari, tenuto conto di tutte le altre garanzie procedurali previste dal diritto nazionale, una volta che queste ultime garantiscono l'efficacia del diritto di ricorso.

67 Per quanto concerne tali altre garanzie procedurali, il giudice del rinvio precisa, in particolare, che chiunque intenda verificare che nessuna tecnica di informazione è applicata in maniera irregolare nei suoi confronti può adire una sezione specializzata del Conseil d'État (Consiglio di Stato), cui compete verificare, alla luce degli elementi che le sono stati comunicati al di fuori della procedura in contraddittorio, se il ricorrente sia stato oggetto di una tecnica e se quest'ultima sia stata attuata in conformità con il libro VIII del CSI. I poteri conferiti a tale sezione per istruire i ricorsi garantirebbero l'effettività del controllo giurisdizionale da essa espletato. Infatti, detta sezione sarebbe competente ad istruire i ricorsi, rilevare d'ufficio ogni illecito da essa constatato e ordinare all'amministrazione di adottare tutte le misure utili per far fronte agli illeciti accertati. Inoltre, spetterebbe alla Commissione nazionale di controllo delle tecniche di informazione verificare che le tecniche di raccolta delle informazioni siano applicate, sul territorio nazionale, nel rispetto degli obblighi risultanti dal CSI. Pertanto, il fatto che le disposizioni legislative di cui al procedimento principale non prevedano la notifica agli interessati delle misure di sorveglianza cui sono stati sottoposti, non integrerebbe, di per sé, una violazione eccessiva del diritto al rispetto della vita privata.

68 In tale contesto, il Conseil d'État (Consiglio di Stato) ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Se l'obbligo di conservazione generalizzata e indifferenziata, imposto ai fornitori sulla base delle disposizioni autorizzative di cui all'articolo 15, paragrafo 1, della direttiva [2002/58], debba essere considerato, in un contesto caratterizzato da minacce gravi e persistenti alla sicurezza nazionale, e

in particolare dal rischio terroristico, come un'ingerenza giustificata dal diritto alla sicurezza garantito dall'articolo 6 della [Carta] e dalle esigenze di sicurezza nazionale, la cui responsabilità è rimessa, a norma dell'articolo 4 [TUE], unicamente agli Stati membri.

2) Se la direttiva [2002/58], letta alla luce della [Carta], debba essere interpretata nel senso che essa autorizza misure legislative, quali la raccolta in tempo reale di dati sul traffico e sull'ubicazione di persone determinate, che, pur incidendo sui diritti e sugli obblighi dei fornitori di un servizio di comunicazioni elettroniche, non per questo impone loro uno specifico obbligo di conservazione dei loro dati.

3) Se la direttiva [2002/58], letta alla luce della [Carta], debba essere interpretata nel senso che essa subordina sempre la regolarità delle procedure di raccolta dei dati di connessione a un obbligo di informazione degli interessati ove tale informazione non sia suscettibile di compromettere le indagini condotte dalle autorità competenti o se tali procedure possano essere considerate regolari, tenuto conto di tutte le altre garanzie procedurali esistenti, una volta che queste ultime garantiscono l'efficacia del diritto di ricorso».

Causa C-512/18

69 Mediante atto introduttivo del 1° settembre 2015, la French Data Network, la Quadrature du Net e la Fédération des fournisseurs d'accès à Internet associatifs hanno adito il Conseil d'État (Consiglio di Stato) con un ricorso diretto all'annullamento della decisione implicita di rigetto scaturita dal silenzio tenuto dal Primo ministro sulla loro domanda di abrogazione dell'articolo R. 10-13 del CPCE e del decreto n. 2011-219, lamentando, in particolare, che tali disposizioni violerebbero l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 della Carta. La Privacy International e il Center for Democracy and Technology sono stati autorizzati ad intervenire nel procedimento principale.

70 Per quanto riguarda l'articolo R. 10-13 del CPCE e l'obbligo di conservazione generalizzata e indifferenziata dei dati relativi alle comunicazioni ivi previsto, il giudice del rinvio, che esprime considerazioni analoghe a quelle esposte nell'ambito della causa C-511/18, osserva che una siffatta conservazione consente all'autorità giudiziaria di accedere ai dati relativi alle comunicazioni che una persona ha effettuato prima di essere sospettata di aver commesso un reato, di modo che tale conservazione presenta un'utilità senza precedenti per la ricerca, l'accertamento e il perseguimento dei reati.

71 Per quanto concerne il decreto n. 2011-219, il giudice del rinvio ritiene che l'articolo 6, paragrafo II, della LCEN, che impone un obbligo di detenere e conservare i soli dati relativi alla creazione di contenuto, non ricada nel campo di applicazione della direttiva 2002/58, essendo quest'ultimo circoscritto, conformemente all'articolo 3, paragrafo 1, di detta direttiva, alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nell'Unione, bensì nel campo di applicazione della direttiva 2000/31.

72 Detto giudice ritiene tuttavia che dall'articolo 15, paragrafi 1 e 2, della direttiva 2000/31 risulti che quest'ultima non prevede, in via di principio, un divieto di conservazione dei dati relativi alla creazione di contenuto cui sia possibile derogare unicamente in via di eccezione. Pertanto, si porrebbe la questione se gli articoli 12, 14 e 15 di detta direttiva, letti alla luce degli articoli da 6 a 8 e 11 e dell'articolo 52, paragrafo 1, della Carta, debbano essere interpretati nel senso che consentono a uno Stato membro di prevedere una normativa nazionale, quale l'articolo 6, paragrafo II, della LCEN, che imponga alle persone interessate di conservare i dati con modalità tali da consentire l'identificazione di chiunque abbia contribuito alla creazione del contenuto o di uno dei contenuti dei servizi da esse forniti al fine di permettere all'autorità giudiziaria, se del caso, di richiederne la comunicazione per ottenere il rispetto delle norme in materia di responsabilità civile o penale.

73 In tale contesto, il Conseil d'État (Consiglio di Stato) ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Se, tenuto conto in particolare delle salvaguardie e dei controlli che accompagnano poi la raccolta e l'utilizzo dei dati di connessione di cui trattasi, l'obbligo di conservazione generalizzata e indifferenziata, imposto ai fornitori sulla base delle disposizioni autorizzative di cui all'articolo 15, paragrafo 1, della direttiva [2002/58], debba essere considerato come un'ingerenza giustificata dal diritto alla sicurezza garantito dall'articolo 6 della [Carta] e dalle esigenze di sicurezza nazionale, la cui responsabilità è rimessa, a norma dell'articolo 4 [TUE], unicamente agli Stati membri.

2) Se le disposizioni della direttiva [2000/31], lette alla luce degli articoli 6, 7, 8 e 11 e dell'articolo 52, paragrafo 1, della [Carta], debbano essere interpretate nel senso che esse consentono a uno Stato di prevedere una normativa nazionale che imponga alle persone la cui attività consiste nell'offrire al pubblico un accesso a servizi di comunicazione online e alle persone fisiche o giuridiche che garantiscono, anche a titolo gratuito, mediante la messa a disposizione del pubblico tramite servizi di comunicazione al pubblico online, l'archiviazione di segnali, scritti, immagini, suoni o messaggi di qualsiasi natura forniti dai destinatari di detti servizi, di conservare i dati con modalità tali da consentire l'identificazione di chiunque abbia contribuito alla creazione del contenuto o di uno dei contenuti dei servizi da esse prestati al fine di permettere all'autorità giudiziaria, se del caso, di richiederne la comunicazione per ottenere il rispetto delle norme in materia di responsabilità civile o penale».

Causa C-520/18

74 Mediante atti introduttivi del 10 gennaio, 16 gennaio, 17 gennaio e 18 gennaio 2017, riuniti nel procedimento principale, l'Ordre des barreaux francophones et germanophone, l'Académie Fiscale ASBL e UA, la Liga voor Mensenrechten ASBL e la Ligue des droits de l'Homme ASBL nonché VZ, WY e XX hanno proposto dinanzi alla Cour constitutionnelle (Corte costituzionale, Belgio) ricorsi diretti all'annullamento della legge del 29 maggio 2016, lamentando che quest'ultima violerebbe 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, adottato dall'Assemblea generale delle Nazioni Unite il 16 dicembre 1966 ed entrato in vigore il 23 marzo 1976, i principi generali di certezza del diritto, di proporzionalità e di autodeterminazione in materia di informazione nonché l'articolo 5, paragrafo 4, TUE.

75 A sostegno dei loro ricorsi, i ricorrenti nel procedimento principale fanno valere, in sostanza, che l'illegittimità della legge del 29 maggio 2016 deriva in particolare dal fatto che quest'ultima eccede i limiti dello stretto necessario e non prevede garanzie di tutela sufficienti. In particolare, né le sue disposizioni relative alla conservazione dei dati né quelle che disciplinano l'accesso delle autorità ai dati conservati risponderebbero ai requisiti risultanti dalla sentenza dell'8 aprile 2014, Digital Rights Ireland e a. (C-293/12 e C-594/12; in prosieguo: la «sentenza Digital Rights», EU:C:2014:238), e dalla sentenza del 21 dicembre 2016, Tele2 (C-203/15 e C-698/15, EU:C:2016:970). Infatti, dette disposizioni comporterebbero il rischio che siano stabiliti profili di personalità, con i conseguenti possibili abusi da parte delle autorità competenti, e non prevedrebbero neppure un livello adeguato di sicurezza e di protezione dei dati conservati. Infine, tale legge si applicherebbe a soggetti tenuti al segreto professionale e a soggetti che hanno un obbligo di riservatezza, e riguarderebbe dati di comunicazione sensibili, di carattere personale, senza comportare specifiche garanzie al fine di proteggere questi ultimi dati.

76 Il giudice del rinvio rileva che i dati che devono conservare i fornitori di servizi di telefonia, compresi quelli via Internet, di accesso a Internet e di posta elettronica su Internet nonché gli operatori che forniscono reti pubbliche di comunicazione elettronica, ai sensi della legge del 29 maggio 2016, sono

identici a quelli elencati dalla direttiva 2006/24/CE 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 e che modifica la direttiva 2002/58/CE (GU 2006, L 105, pag. 54), senza che sia prevista alcuna distinzione quanto alle persone interessate o in funzione dell'obiettivo perseguito. Sotto quest'ultimo profilo, detto giudice precisa che l'obiettivo che il legislatore persegue per mezzo di tale legge non riguarda unicamente la lotta contro il terrorismo e la pornografia minorile, ma anche la possibilità di utilizzare i dati conservati in un'ampia gamma di situazioni nell'ambito delle indagini penali. Inoltre, il giudice del rinvio osserva che dalla relazione illustrativa di detta legge risulta che il legislatore nazionale non ha considerato che fosse possibile, alla luce dell'obiettivo perseguito, introdurre un obbligo di conservazione mirato e differenziato e ha scelto di dotare l'obbligo di conservazione generale e differenziato di garanzie rigorose, tanto sul piano dei dati conservati quanto sul piano dell'accesso ai medesimi, allo scopo di limitare al minimo l'ingerenza nel diritto alla protezione della vita privata.

77 Il giudice del rinvio aggiunge che l'articolo 126, paragrafo 2, punti 1° e 2°, della legge del 13 giugno 2005, nella versione risultante dalla legge del 29 maggio 2016, prevede le condizioni alle quali, rispettivamente, le autorità giudiziarie e i servizi di intelligence e di sicurezza possono ottenere l'accesso ai dati conservati, di modo che l'esame della legittimità di tale legge alla luce dei requisiti del diritto dell'Unione dovrebbe essere sospeso fino a quando la Corte non si sia pronunciata in due procedimenti pregiudiziali, pendenti dinanzi ad essa, relativi a un siffatto accesso.

78 Infine, il giudice del rinvio rileva che la legge del 29 maggio 2016 intende consentire un accertamento penale e un regime sanzionatorio effettivi per gli abusi sessuali sui minori e rendere possibile l'identificazione dell'autore di un tale reato anche quando sono impiegati mezzi di comunicazione elettronica. Nel corso del procedimento dinanzi ad esso sarebbe stata richiamata l'attenzione a tale proposito sugli obblighi positivi che derivano dagli articoli 3 e 8 della CEDU. Detti obblighi potrebbero ugualmente derivare dalle disposizioni corrispondenti della Carta, le quali potrebbero avere ripercussioni sull'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58.

79 In tale contesto, la Cour constitutionnelle (Corte costituzionale) ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Se l'articolo 15, paragrafo 1, della direttiva [2002/58], letto in combinato disposto con il diritto alla sicurezza, quale garantito dall'articolo 6 della [Carta], e con il diritto al rispetto dei dati di carattere personale, quale garantito dagli articoli 7, 8 e 52, paragrafo 1, della [Carta], debba essere interpretato nel senso che esso osta a una normativa nazionale, come quella di cui trattasi nel procedimento principale, che prevede un obbligo generale per gli operatori e i fornitori di servizi di comunicazione elettronica di conservare i dati relativi al traffico e all'ubicazione ai sensi della direttiva [2002/58], da essi generati o trattati nel quadro della fornitura di detti servizi, normativa nazionale che non si prefigge come obiettivo esclusivamente la ricerca, l'accertamento e il perseguimento di fatti di criminalità grave, ma anche la garanzia della sicurezza nazionale, della difesa del territorio e della sicurezza pubblica, la ricerca, l'accertamento e il perseguimento di fatti diversi da quelli di criminalità grave o la prevenzione dell'uso non autorizzato dei sistemi di comunicazione elettronica, oppure la realizzazione di altro obiettivo identificato dall'articolo 23, paragrafo 1, del regolamento [2016/679], e che è inoltre soggetta alle garanzie che essa stessa specifica per quanto concerne la conservazione dei dati e la loro consultazione.

2) Se l'articolo 15, paragrafo 1, della direttiva [2002/58], in combinato disposto con gli articoli 4, 7, 8, 11 e 52, paragrafo 1, della [Carta], debba essere interpretato nel senso che esso osta a una normativa nazionale, come quella di cui trattasi nel procedimento principale, che prevede un obbligo generale per gli operatori e i fornitori di servizi di comunicazione elettronica di conservare i dati relativi al traffico e all'ubicazione ai sensi della direttiva [2002/58], da essi generati o trattati nel quadro della fornitura di detti servizi, se tale normativa ha segnatamente come obiettivo quello di dare attuazione agli obblighi positivi che gravano sulle autorità in forza degli articoli 4 e [7] della

Carta, ovvero di prevedere un quadro normativo che permetta lo svolgimento di indagini penali preliminari effettive e una repressione effettiva degli abusi sessuali sui minori e che permetta in concreto di identificare l'autore del reato anche quando sono impiegati mezzi di comunicazione elettronica.

3) Qualora, sulla base delle risposte fornite alla prima o alla seconda questione pregiudiziale, la Cour constitutionnelle [Corte costituzionale] giunga alla conclusione che la legge impugnata viola uno o più fra gli obblighi derivanti dalle disposizioni che tali questioni menzionano, se possano essere mantenuti provvisoriamente gli effetti della legge del [29 maggio 2016] al fine di evitare una situazione di incertezza giuridica e di permettere che i dati raccolti e conservati in precedenza possano ancora essere utilizzati per il raggiungimento degli obiettivi previsti dalla legge».

Sul procedimento dinanzi alla Corte

80 Con decisione del presidente della Corte del 25 settembre 2018, le cause C-511/18 e C-512/18 sono state riunite ai fini delle fasi scritta e orale del procedimento, nonché della sentenza. La causa C-520/18 è stata riunita a tali cause con decisione del presidente della Corte del 9 luglio 2020 ai fini della sentenza.

Sulle questioni pregiudiziali

Sulle prime questioni nelle cause C-511/18 e C-512/18 e sulle questioni prima e seconda nella causa C-520/18

81 Con le prime questioni nelle cause C-511/18 e C-512/18 e con le questioni prima e seconda nella causa C-520/18, che occorre esaminare congiuntamente, i giudici del rinvio chiedono, in sostanza, se l'articolo 15, paragrafo 1, della direttiva 2002/58 debba essere interpretato nel senso che osta a una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica, ai fini previsti da tale articolo 15, paragrafo 1, una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione.

Osservazioni preliminari

82 Dagli atti di causa a disposizione della Corte risulta che le normative di cui trattasi nei procedimenti principali disciplinano tutti i mezzi di comunicazione elettronica e ricomprendono tutti gli utenti di tali mezzi, senza che sia operata al riguardo alcuna distinzione o eccezione. Inoltre, i dati che tali normative impongono ai fornitori di servizi di comunicazione elettronica di conservare sono, in particolare, quelli necessari per individuare l'origine e la destinazione di una comunicazione, determinare la data, l'ora, la durata e il tipo di comunicazione, identificare lo strumento di comunicazione utilizzato nonché localizzare le apparecchiature terminali e le comunicazioni, dati tra i quali figurano, in particolare, il nome e l'indirizzo dell'utente, i numeri di telefono del chiamante e del chiamato nonché l'indirizzo IP per i servizi Internet. Per contro, detti dati non includono il contenuto delle comunicazioni interessate.

83 Pertanto, i dati che, in forza delle normative nazionali di cui ai procedimenti principali, devono essere conservati per un anno consentono, in particolare, di sapere quale sia la persona con cui ha comunicato l'utente di un mezzo di comunicazione elettronica e con quale mezzo è stata effettuata tale comunicazione, di determinare la data, l'ora e la durata delle comunicazioni e delle connessioni a Internet nonché il luogo a partire dal quale esse sono state effettuate, e di conoscere l'ubicazione delle apparecchiature terminali senza che sia necessariamente instradata una comunicazione. Inoltre, essi consentono di determinare la frequenza delle comunicazioni dell'utente con talune persone durante

un periodo determinato. Infine, per quanto riguarda la normativa nazionale di cui trattasi nelle cause C-511/18 e C-512/18, sembra che essa, dal momento che si applica anche ai dati relativi alla trasmissione delle comunicazioni elettroniche attraverso le reti, permetta altresì di identificare la natura delle informazioni consultate online.

84 Quanto alle finalità perseguite, si deve rilevare che le normative di cui trattasi nelle cause C-511/18 e C-512/18 riguardano, tra l'altro, la ricerca, l'accertamento e il perseguimento dei reati in generale, l'indipendenza nazionale, l'integrità del territorio e la difesa nazionale, gli interessi superiori della politica estera, l'esecuzione degli impegni europei ed internazionali della Francia, gli interessi superiori economici, industriali e scientifici della Francia, nonché la prevenzione del terrorismo, degli attentati alla forma repubblicana delle istituzioni e delle violenze collettive tali da compromettere gravemente il mantenimento della legge e dell'ordine. Per quanto concerne la normativa di cui trattasi nella causa C-520/18, essa ha come obiettivo, tra l'altro, la ricerca, l'accertamento e il perseguimento di reati nonché la salvaguardia della sicurezza nazionale, della difesa del territorio e della sicurezza pubblica.

85 I giudici del rinvio si interrogano, in particolare, in merito alle eventuali incidenze del diritto alla sicurezza sancito dall'articolo 6 della Carta sull'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58. Analogamente, si chiedono se l'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta che comporta la conservazione dei dati prevista dalle normative di cui trattasi nei procedimenti principali possa essere considerata giustificata, tenuto conto dell'esistenza di norme che limitano l'accesso delle autorità nazionali ai dati conservati. Inoltre, secondo il Conseil d'État (Consiglio di Stato), poiché tale questione si pone in un contesto segnato da minacce gravi e persistenti alla sicurezza nazionale, deve essere valutata anche alla luce dell'articolo 4, paragrafo 2, TUE. La Cour constitutionnelle (Corte costituzionale), dal canto suo, sottolinea che la normativa nazionale di cui trattasi nella causa C-520/18 dà attuazione anche ad obblighi positivi derivanti dagli articoli 4 e 7 della Carta, che consistono nel prevedere un quadro normativo che permetta la repressione effettiva degli abusi sessuali sui minori.

86 Mentre sia il Conseil d'État (Consiglio di Stato) che la Cour constitutionnelle (Corte costituzionale) muovono dalla premessa secondo cui le normative nazionali di cui trattasi nei procedimenti principali, che disciplinano la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione nonché l'accesso a tali dati da parte delle autorità nazionali ai fini previsti dall'articolo 15, paragrafo 1, della direttiva 2002/58, quali la salvaguardia della sicurezza nazionale, rientrano nell'ambito di applicazione di detta direttiva, alcune delle parti nei procedimenti principali e alcuni degli Stati membri che hanno presentato osservazioni scritte alla Corte esprimono opinioni divergenti al riguardo, in particolare per quanto concerne l'interpretazione dell'articolo 1, paragrafo 3, della medesima direttiva. Occorre quindi esaminare, anzitutto, se le summenzionate normative rientrino nell'ambito di applicazione di tale direttiva.

Sull'ambito di applicazione della direttiva 2002/58

87 La Quadrature del Net, la Fédération des fournisseurs d'accès à Internet associatifs, la Igwan.net, la Privacy International e il Center for Democracy and Technology deducono in sostanza, richiamando al riguardo la giurisprudenza della Corte relativa all'ambito di applicazione della direttiva 2002/58, che tanto la conservazione dei dati quanto l'accesso ai dati conservati rientrano in tale ambito di applicazione, indipendentemente dalla circostanza che detto accesso avvenga in tempo differito o in tempo reale. Infatti, poiché l'obiettivo di salvaguardia della sicurezza nazionale è espressamente menzionato all'articolo 15, paragrafo 1, della direttiva citata, il perseguimento di questo obiettivo non comporterebbe l'inapplicabilità della suddetta direttiva. L'articolo 4, paragrafo 2, TUE, richiamato dai giudici del rinvio, non inficerebbe tale valutazione.

88 Per quanto riguarda le misure di intelligence che le autorità francesi competenti applicano direttamente senza disciplinare l'attività dei fornitori di servizi di comunicazione elettronica imponendo loro obblighi specifici, il Center for Democracy and Technology osserva che tali misure rientrano necessariamente nell'ambito di applicazione della direttiva 2002/58 e in quello della Carta, in quanto costituiscono deroghe al principio di riservatezza garantito dall'articolo 5 di detta direttiva. Le misure in parola dovrebbero quindi rispettare i requisiti risultanti dall'articolo 15, paragrafo 1, della stessa.

89 Per contro, i governi francese, ceco ed estone, l'Irlanda, nonché i governi cipriota, polacco, svedese, ungherese e del Regno Unito sostengono, in sostanza, che la direttiva 2002/58 non si applica a normative nazionali come quelle di cui trattasi nei procedimenti principali, nella misura in cui esse sono finalizzate alla salvaguardia della sicurezza nazionale. Le attività dei servizi di intelligence, dal momento che riguardano il mantenimento dell'ordine pubblico nonché la salvaguardia della sicurezza interna e dell'integrità territoriale, rientrerebbero nelle funzioni essenziali degli Stati membri e, di conseguenza, sarebbero di esclusiva competenza di questi ultimi, come dimostrerebbe in particolare l'articolo 4, paragrafo 2, terza frase, TUE.

90 Detti governi e l'Irlanda richiamano inoltre l'articolo 1, paragrafo 3, della direttiva 2002/58, che esclude dall'ambito di applicazione della stessa, analogamente a quanto già prevedeva l'articolo 3, paragrafo 2, primo trattino, della direttiva 95/46, le attività concernenti la sicurezza pubblica, la difesa e la sicurezza dello Stato. Essi si basano al riguardo sull'interpretazione di quest'ultima disposizione esposta nella sentenza del 30 maggio 2006, Parlamento/Consiglio e Commissione (C-317/04 e C-318/04, EU:C:2006:346).

91 A tale proposito, occorre ricordare che, a termini del suo articolo 1, paragrafo 1, la direttiva 2002/58 prevede, tra l'altro, l'armonizzazione delle disposizioni nazionali necessarie per assicurare un livello equivalente di tutela dei diritti e delle libertà fondamentali, e in particolare del diritto alla vita privata e alla riservatezza, con riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche.

92 L'articolo 1, paragrafo 3, di tale direttiva esclude dall'ambito di applicazione della stessa le «attività dello Stato» nei settori ivi indicati, tra le quali figurano le attività dello Stato in settori del diritto penale e quelle riguardanti la sicurezza pubblica, la difesa e la sicurezza dello Stato, compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato. Le attività così menzionate a titolo esemplificativo sono, in tutti i casi, attività proprie degli Stati o delle autorità statali, estranee ai settori di attività dei privati (sentenza del 2 ottobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punto 32 e giurisprudenza citata).

93 Inoltre, l'articolo 3 della direttiva 2002/58 enuncia che detta direttiva si applica al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche nell'Unione, comprese le reti di comunicazione pubbliche che supportano i dispositivi di raccolta e di identificazione dei dati (in prosieguo: i «servizi di comunicazione elettronica»). Pertanto, la citata direttiva deve essere considerata come disciplinante le attività dei fornitori di tali servizi (sentenza del 2 ottobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punto 33 e giurisprudenza citata).

94 In tale contesto, l'articolo 15, paragrafo 1, della direttiva 2002/58 autorizza gli Stati membri ad adottare, nel rispetto delle condizioni da esso previste, «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 [citata] direttiva» (sentenza del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punto 71).

95 Orbene, l'articolo 15, paragrafo 1, della direttiva 2002/58 presuppone necessariamente che le misure legislative nazionali ivi indicate rientrino nell'ambito di applicazione della stessa, poiché quest'ultima autorizza espressamente gli Stati membri ad adottarle solamente nel rispetto delle condizioni che essa

prevede. Inoltre, siffatte misure disciplinano, per le finalità menzionate in tale disposizione, l'attività dei fornitori di servizi di comunicazione elettronica (sentenza del 2 ottobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punto 34 e giurisprudenza citata).

96 Segnatamente alla luce di tali considerazioni la Corte ha dichiarato che l'articolo 15, paragrafo 1, letto in combinato disposto con l'articolo 3, della direttiva 2002/58 deve essere interpretato nel senso che rientra nell'ambito di applicazione di detta direttiva non solo una misura legislativa che impone ai fornitori di servizi di comunicazione elettronica di conservare i dati relativi al traffico e i dati relativi all'ubicazione, ma anche una misura legislativa che impone loro di accordare alle autorità nazionali competenti l'accesso a tali dati. Infatti, misure legislative di tal genere implicano necessariamente un trattamento, da parte dei fornitori suddetti, di questi dati e non possono, nei limiti in cui disciplinano le attività di questi stessi fornitori, essere considerate come attività proprie degli Stati, di cui all'articolo 1, paragrafo 3, della menzionata direttiva (v., in tal senso, sentenza del 2 ottobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punti 35 e 37 e giurisprudenza citata).

97 Inoltre, alla luce delle considerazioni svolte al punto 95 della presente sentenza e dell'economia generale della direttiva 2002/58, un'interpretazione di detta direttiva secondo la quale le disposizioni legislative di cui al suo articolo 15, paragrafo 1, sarebbero escluse dall'ambito di applicazione della stessa, in quanto le finalità che siffatte disposizioni devono soddisfare coincidono sostanzialmente con le finalità perseguite dalle attività contemplate dall'articolo 1, paragrafo 3, della medesima direttiva, priverebbe tale articolo 15, paragrafo 1, di qualsiasi effetto utile (v., in tal senso, sentenza del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punti 72 e 73).

98 Pertanto, la nozione di «attività» riportata all'articolo 1, paragrafo 3, della direttiva 2002/58 non può, come rilevato in sostanza dall'avvocato generale al paragrafo 75 delle conclusioni nelle cause riunite La Quadrature du Net e a. (C-511/18 e C-512/18, EU:C:2020:6), essere interpretata nel senso che comprende le disposizioni legislative menzionate all'articolo 15, paragrafo 1, di tale direttiva.

99 Le disposizioni dell'articolo 4, paragrafo 2, TUE, alle quali hanno fatto riferimento i governi menzionati al punto 89 della presente sentenza, non valgono ad inficiare tale conclusione. Infatti, conformemente alla giurisprudenza costante della Corte, sebbene spetti agli Stati membri definire gli interessi essenziali della propria sicurezza e decidere le misure idonee a garantire la loro sicurezza interna ed esterna, la mera circostanza che una misura nazionale sia stata adottata a fini di salvaguardia della sicurezza nazionale non può comportare l'inapplicabilità del diritto dell'Unione e dispensare gli Stati membri dal necessario rispetto di tale diritto [v., in tal senso, sentenze del 4 giugno 2013, ZZ, C-300/11, EU:C:2013:363, punto 38; del 20 marzo 2018, Commissione/Austria (Tipografia di Stato), C-187/16, EU:C:2018:194, punti 75 e 76, e del 2 aprile 2020, Commissione/Polonia, Ungheria e Repubblica ceca (Meccanismo temporaneo di ricollocazione di richiedenti protezione internazionale), C-715/17, C-718/17 e C-719/17, EU:C:2020:257, punti 143 e 170].

100 È vero che, nella sentenza del 30 maggio 2006, Parlamento/Consiglio e Commissione (C-317/04 e C-318/04, EU:C:2006:346, punti da 56 a 59), la Corte ha dichiarato che il trasferimento dei dati personali da parte di vettori aerei ad autorità pubbliche di uno Stato terzo a fini di prevenzione nonché di lotta contro il terrorismo e altri reati gravi non ricadeva, in forza dell'articolo 3, paragrafo 2, primo trattino, della direttiva 95/46, nell'ambito di applicazione di detta direttiva, in quanto tale trasferimento rientrava in un ambito istituito dai poteri pubblici attinente alla pubblica sicurezza.

101 Tuttavia, alla luce delle considerazioni svolte ai punti 93, 95 e 96 della presente sentenza, questa giurisprudenza non può essere applicata all'interpretazione dell'articolo 1, paragrafo 3, della direttiva 2002/58. Infatti, come ha rilevato, in sostanza, l'avvocato generale ai paragrafi da 70 a 72 delle sue conclusioni nelle cause riunite La Quadrature du Net e a. (C-511/18 e C-512/18, EU:C:2020:6), l'articolo 3, paragrafo 2, primo trattino, della direttiva 95/46, al quale si riferisce detta giurisprudenza, escludeva dall'ambito di applicazione di quest'ultima direttiva, in generale, i «trattamenti aventi come

oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato», senza operare distinzioni a seconda dell'autore del trattamento dei dati in questione. Per contro, nell'ambito dell'interpretazione dell'articolo 1, paragrafo 3, della direttiva 2002/58, una siffatta distinzione appare necessaria. Infatti, come risulta dai punti da 94 a 97 della presente sentenza, tutti i trattamenti di dati personali effettuati dai fornitori di servizi di comunicazione elettronica ricadono nell'ambito di applicazione di detta direttiva, compresi i trattamenti derivanti da obblighi loro imposti dai pubblici poteri, mentre questi ultimi trattamenti potevano, se del caso, rientrare nell'eccezione prevista all'articolo 3, paragrafo 2, primo trattino, della direttiva 95/46, tenuto conto della formulazione più ampia di tale disposizione, che riguardava tutti i trattamenti, indipendentemente dal loro autore, aventi come oggetto la pubblica sicurezza, la difesa o la sicurezza dello Stato.

102 Inoltre, occorre rilevare che la direttiva 95/46 in discussione nella causa che ha dato luogo alla sentenza del 30 maggio 2006, Parlamento/Consiglio e Commissione (C-317/04 e C-318/04, EU:C:2006:346), è stata, in forza dell'articolo 94, paragrafo 1, del regolamento 2016/679, abrogata e sostituita da quest'ultimo, a decorrere dal 25 maggio 2018. Orbene, sebbene detto regolamento precisi, all'articolo 2, paragrafo 2, lettera d), che esso non si applica ai trattamenti effettuati «dalle autorità competenti» a fini, in particolare, di prevenzione ed accertamento dei reati, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse, dall'articolo 23, paragrafo 1, lettere d) e h), del medesimo regolamento risulta che i trattamenti di dati personali effettuati a questi stessi fini da soggetti privati rientrano nel suo ambito di applicazione. Ne consegue che la suesposta interpretazione dell'articolo 1, paragrafo 3, dell'articolo 3 e dell'articolo 15, paragrafo 1, della direttiva 2002/58 è coerente con la delimitazione dell'ambito di applicazione del regolamento 2016/679 che tale direttiva completa e precisa.

103 Per contro, quando gli Stati membri attuano direttamente misure che derogano alla riservatezza delle comunicazioni elettroniche, senza imporre obblighi di trattamento ai fornitori di detti servizi di comunicazione, la protezione dei dati delle persone interessate non ricade nell'ambito della direttiva 2002/58, bensì unicamente in quello del diritto nazionale, fatta salva l'applicazione della 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 (GU 2016, L 119, pag. 89), di modo che le misure in questione devono rispettare in particolare il diritto nazionale di rango costituzionale e i requisiti della CEDU.

104 Dalle suesposte considerazioni risulta che 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, quali le normative di cui trattasi nei procedimenti principali, rientra nell'ambito di applicazione della direttiva 2002/58.

Sull'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58

105 Va ricordato, in via preliminare, che, secondo una giurisprudenza costante, ai fini dell'interpretazione di una norma del diritto dell'Unione non si deve soltanto fare riferimento al tenore letterale della stessa, ma anche tenere conto del suo contesto e degli scopi perseguiti dalla normativa di cui essa fa parte e prendere in considerazione, in particolare, la genesi di tale normativa (v., in tal senso, sentenza del 17 aprile 2018, Egenberger, C-414/16, EU:C:2018:257, punto 44).

106 La direttiva 2002/58 è finalizzata, come risulta in particolare dai suoi considerando 6 e 7, a proteggere gli utenti dei servizi di comunicazione elettronica dai pericoli per i loro dati personali e la loro vita privata derivanti dalle nuove tecnologie e, in particolare, dall'accresciuta capacità di memorizzazione e di trattamento automatizzati di dati. In particolare, detta direttiva mira, come enunciato dal suo considerando 2, a garantire il pieno rispetto dei diritti di cui agli articoli 7 e 8 della Carta. A tale

proposito, dalla relazione alla proposta di direttiva del Parlamento europeo e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche [COM(2000) 385 definitivo], all'origine della direttiva 2002/58, risulta che il legislatore dell'Unione ha inteso «assicurare un elevato livello di tutela dei dati personali e della vita privata per tutti i servizi di comunicazione elettronica, indipendentemente dalla tecnologia da essi usata».

107 A tal fine, l'articolo 5, paragrafo 1, della direttiva 2002/58 sancisce il principio di riservatezza sia delle comunicazioni elettroniche sia dei dati relativi al traffico a queste correlati e implica, in particolare, il divieto imposto, in linea di principio, a qualsiasi persona diversa dagli utenti di memorizzare senza il loro consenso tali comunicazioni e dati.

108 Per quanto riguarda, in particolare, il trattamento e la memorizzazione dei dati relativi al traffico da parte dei fornitori di servizi di comunicazione elettronica, dall'articolo 6 nonché dai considerando 22 e 26 della direttiva 2002/58 risulta che un siffatto trattamento è autorizzato soltanto nella misura e per la durata necessaria per la commercializzazione dei servizi, per la fatturazione degli stessi e per la fornitura di servizi a valore aggiunto. Una volta terminato tale periodo, i dati che sono stati trattati e memorizzati devono essere cancellati o resi anonimi. Quanto ai dati relativi all'ubicazione diversi dai dati relativi al traffico, l'articolo 9, paragrafo 1, di detta direttiva stabilisce che tali dati possono essere trattati soltanto in presenza di determinate condizioni e dopo essere stati resi anonimi oppure con il consenso degli utenti o degli abbonati (sentenza del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punto 86 e giurisprudenza citata).

109 Pertanto, adottando tale direttiva, il legislatore dell'Unione ha concretizzato i diritti sanciti dagli articoli 7 e 8 della Carta, di modo che gli utenti dei mezzi di comunicazione elettronica hanno il diritto di attendersi, in linea di principio, che le loro comunicazioni e i dati a queste correlati, in mancanza del loro consenso, rimangano anonimi e non possano essere registrati.

110 Tuttavia, l'articolo 15, paragrafo 1, della direttiva 2002/58 consente agli Stati membri di introdurre eccezioni all'obbligo di principio, enunciato all'articolo 5, paragrafo 1, di tale direttiva, di garantire la riservatezza dei dati personali nonché ai corrispondenti obblighi, menzionati in particolare agli articoli 6 e 9 di detta direttiva, qualora tale restrizione costituisca una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale, della difesa e 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 che prevedano la conservazione dei dati per un periodo di tempo limitato, qualora ciò sia giustificato da uno dei suddetti motivi.

111 Ciò premesso, la facoltà di derogare ai diritti e agli obblighi previsti dagli articoli 5, 6 e 9 della direttiva 2002/58 non può giustificare che la deroga all'obbligo di principio di garantire la riservatezza delle comunicazioni elettroniche e dei dati a queste correlati e, in particolare, al divieto di memorizzare tali dati, espressamente previsto all'articolo 5 di detta direttiva, divenga la regola (v., in tal senso, sentenza del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punti 89 e 104).

112 Quanto agli obiettivi idonei a giustificare una limitazione dei diritti e degli obblighi previsti, in particolare, dagli articoli 5, 6 e 9 della direttiva 2002/58, la Corte ha già dichiarato che l'elenco degli obiettivi di cui all'articolo 15, paragrafo 1, prima frase, di tale direttiva ha carattere tassativo, di modo che una misura legislativa adottata ai sensi di detta disposizione deve rispondere in modo effettivo e rigoroso ad uno di questi obiettivi (v., in tal senso, sentenza del 2 ottobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punto 52 e giurisprudenza citata).

113 Inoltre, dall'articolo 15, paragrafo 1, terza frase, della direttiva 2002/58 risulta che gli Stati membri 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, la Corte ha già dichiarato che l'obbligo imposto da uno Stato membro ai fornitori di servizi di comunicazione elettronica, in forza di una normativa nazionale, di conservare i dati relativi al traffico al fine di renderli, se del caso, accessibili alle autorità nazionali competenti solleva questioni riguardanti il rispetto non soltanto degli articoli 7 e 8 della Carta, relativi, rispettivamente, alla tutela della vita privata e alla protezione dei dati personali, ma anche dell'articolo 11 della Carta, relativo alla libertà di espressione (v., in tal senso, sentenza dell'8 aprile 2014, Digital Rights, C-293/12 e C-594/12, EU:C:2014:238, punti 25 e 70, e del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punti 91 e 92 e giurisprudenza citata).

114 Pertanto, l'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/85 deve tenere conto dell'importanza sia del diritto al rispetto della vita privata, garantito dall'articolo 7 della Carta, sia del diritto alla protezione dei dati personali, sancito dall'articolo 8 di quest'ultima, quale emerge dalla giurisprudenza della Corte, nonché del diritto alla libertà di espressione, dal momento che tale diritto fondamentale, garantito dall'articolo 11 della Carta, costituisce uno dei fondamenti essenziali di una società democratica e pluralista, facente parte dei valori sui quali, a norma dell'articolo 2 TUE, l'Unione è fondata (v., in tal senso, sentenze del 6 marzo 2001, Connolly/Commissione, C-274/99 P, EU:C:2001:127, punto 39, e del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punto 93 e giurisprudenza citata).

115 Occorre precisare, a tale proposito, che la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione costituisce, di per sé, da un lato, una deroga al divieto, previsto dall'articolo 5, paragrafo 1, della direttiva 2002/58, per qualsiasi persona diversa dagli utenti di memorizzare tali dati e, dall'altro, un'ingerenza nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali, sanciti dagli articoli 7 e 8 della Carta, a prescindere dalla circostanza che le informazioni relative alla vita privata di cui trattasi abbiano o meno un carattere sensibile o che gli interessati abbiano o meno subito eventuali inconvenienti in seguito a siffatta ingerenza [v., in tal senso, parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, EU:C:2017:592, punti 124 e 126 e giurisprudenza citata; v., per analogia, relativamente all'articolo 8 della CEDU, Corte EDU, 30 gennaio 2020, Breyer c. Germania, CE:ECHR:2020:0130JUD005000112, § 81].

116 È del pari irrilevante la circostanza che i dati conservati siano o meno utilizzati successivamente (v., per analogia, relativamente all'articolo 8 della CEDU, Corte EDU, 16 febbraio 2000, Amann c. Svizzera, CE:ECHR:2000:0216JUD002779895, § 69, e 13 febbraio 2020, Trjakovski e Chipovski c. Macedonia del Nord, CE:ECHR:2020:0213JUD005320513, § 51), in quanto l'accesso a tali dati costituisce, a prescindere dall'uso che ne viene fatto in seguito, un'ingerenza distinta nei diritti fondamentali indicati al punto precedente [v., in tal senso, parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, EU:C:2017:592, punti 124 e 126].

117 Questa conclusione risulta tanto più giustificata in quanto i dati relativi al traffico e i dati relativi all'ubicazione possono rivelare informazioni su un numero significativo di aspetti della vita privata degli interessati, comprese informazioni sensibili, quali l'orientamento sessuale, le opinioni politiche, le convinzioni religiose, filosofiche, sociali o di altro tipo nonché lo stato di salute, mentre tali dati beneficiano, peraltro, di una tutela particolare nel diritto dell'Unione. Presi nel loro insieme, tali dati sono idonei a consentire di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono stati conservati, come le abitudini della vita quotidiana, i luoghi di soggiorno permanenti o temporanei, gli spostamenti giornalieri o di altro tipo, le attività esercitate, le relazioni sociali di dette persone e gli ambienti sociali da esse frequentati. In particolare, questi dati forniscono gli strumenti per stabilire il profilo delle persone interessate, informazione tanto sensibile, in rapporto al diritto al rispetto della vita privata, quanto il contenuto stesso delle comunicazioni (v., in tal senso, sentenze dell'8 aprile 2014, Digital Rights, C-293/12 e C-594/12, EU:C:2014:238, punto 27, e del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punto 99).

118 Pertanto, da un lato, la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione a fini di polizia è idoneo, di per sé, a ledere il diritto al rispetto delle comunicazioni, sancito dall'articolo 7 della Carta, e a comportare effetti dissuasivi sull'esercizio da parte degli utenti dei mezzi di comunicazione elettronica della loro libertà di espressione, garantita dall'articolo 11 della Carta (v., in tal senso, sentenze dell'8 aprile 2014, Digital Rights, C-293/12 e C-594/12, EU:C:2014:238, punto 28, e del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punto 101). Orbene, siffatti effetti dissuasivi possono riguardare in particolare le persone le cui comunicazioni sono soggette, secondo le norme nazionali, al segreto professionale e gli informatori le cui attività sono tutelate dalla direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione (GU 2019, L 305, pag. 17). Inoltre, tali effetti sono tanto più gravi quanto maggiori sono il numero e la varietà dei dati conservati.

119 Dall'altro lato, tenuto conto della quantità rilevante di dati relativi al traffico e di dati relativi all'ubicazione che possono essere conservati continuativamente mediante una misura di conservazione generalizzata e indifferenziata nonché del carattere sensibile delle informazioni che tali dati possono fornire, la conservazione di questi da parte dei fornitori di servizi di comunicazione elettronica comporta di per sé rischi di abuso e di accesso illecito.

120 Ciò premesso, l'articolo 15, paragrafo 1, della direttiva 2002/58, laddove consente agli Stati membri di introdurre le deroghe menzionate al punto 110 della presente sentenza, riflette la circostanza che i diritti sanciti dagli articoli 7, 8 e 11 della Carta non appaiono come prerogative assolute, ma vanno considerati alla luce della loro funzione sociale (v., in tal senso, sentenza del 16 luglio 2020, Facebook Ireland e Schrems, C-311/18, EU:C:2020:559, punto 172 e giurisprudenza citata).

121 Infatti, come risulta dall'articolo 52, paragrafo 1, della Carta, quest'ultima ammette limitazioni all'esercizio dei summenzionati diritti, purché tali limitazioni siano previste dalla legge, rispettino il contenuto essenziale di detti diritti e, nel rispetto del principio di proporzionalità, siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

122 Pertanto, l'interpretazione dell'articolo 15, paragrafo 1, della direttiva 2002/58 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 Carta 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.

123 A tal riguardo, l'articolo 6 della Carta, al quale fanno riferimento il Conseil d'État (Consiglio di Stato) e la Cour constitutionnelle (Corte costituzionale), sancisce il diritto di ogni persona non solo alla libertà ma anche alla sicurezza e garantisce diritti corrispondenti a quelli sanciti dall'articolo 5 della CEDU (v., in tal senso, sentenze del 15 febbraio 2016, N., C-601/15 PPU, EU:C:2016:84, punto 47; del 28 luglio 2016, JZ, C-294/16 PPU, EU:C:2016:610, punto 48, e del 19 settembre 2019, Rayonna prokuratura Lom, C-467/18, EU:C:2019:765, punto 42 e giurisprudenza citata).

124 Inoltre, si deve ricordare che l'articolo 52, paragrafo 3, della Carta è inteso ad assicurare la necessaria coerenza tra i diritti contenuti in quest'ultima e i corrispondenti diritti garantiti dalla CEDU, senza che ciò pregiudichi l'autonomia del diritto dell'Unione e della Corte di giustizia dell'Unione europea. Occorre dunque tenere conto dei diritti corrispondenti della CEDU ai fini dell'interpretazione della Carta, in quanto livello minimo di protezione [v., in tal senso, sentenze del 12 febbraio 2019, TC, C-492/18 PPU, EU:C:2019:108, punto 57, e del 21 maggio 2019, Commissione/Ungheria (Usufrutti su terreni agricoli), C-235/17, EU:C:2019:432, punto 72 e giurisprudenza citata].

125 Per quanto riguarda l'articolo 5 della CEDU, che sancisce il «diritto alla libertà» e il «diritto alla sicurezza», esso mira, secondo la giurisprudenza della Corte europea dei diritti dell'uomo, a proteggere l'individuo da qualsiasi privazione arbitraria o ingiustificata della libertà (v., in tal senso,

Corte EDU, 8 marzo 2008, Ladent c. Polonia, CE:ECHR:2008:0318JUD001103603, §§ 45 e 46; 29 marzo 2010, Medvedyev e a. c. Francia, CE:ECHR:2010:0329JUD000339403, §§ 76 e 77, nonché 13 dicembre 2012, El-Masri c. «The former Yugoslav Republic of Macedonia», CE:ECHR:2012:1213JUD003963009, § 239). Tuttavia, poiché tale disposizione riguarda una privazione della libertà commessa da un'autorità pubblica, l'articolo 6 della Carta non può essere interpretato nel senso che impone ai poteri pubblici un obbligo di adottare misure specifiche al fine di reprimere determinati reati.

126 Viceversa, per quanto riguarda, in particolare, la lotta effettiva contro i reati di cui sono vittime i minori e le altre persone vulnerabili, evocata dalla Cour constitutionnelle (Corte costituzionale), occorre sottolineare che obblighi positivi a carico dei pubblici poteri possono risultare dall'articolo 7 della Carta, ai fini dell'adozione di misure giuridiche dirette a tutelare la vita privata e familiare [v., in tal senso, sentenza del 18 giugno 2020, Commissione/Ungheria (Trasparenza associativa), C-78/18, EU:C:2020:476, punto 123 e giurisprudenza citata della Corte europea dei diritti dell'uomo]. Obblighi siffatti possono parimenti derivare da detto articolo 7 per quanto riguarda la protezione del domicilio e delle comunicazioni, nonché dagli articoli 3 e 4 relativamente alla tutela dell'integrità fisica e psichica delle persone e al divieto di tortura e di trattamenti inumani e degradanti.

127 Orbene, di fronte a questi diversi obblighi positivi, occorre procedere al necessario contemperamento dei diversi interessi e diritti in gioco.

128 Infatti, la Corte europea dei diritti dell'uomo ha dichiarato che gli obblighi positivi derivanti dagli articoli 3 e 8 della CEDU, le cui garanzie corrispondenti figurano agli articoli 4 e 7 della Carta, implicano, in particolare, l'adozione di disposizioni sostanziali e procedurali nonché di misure di natura pratica che consentano di contrastare efficacemente i reati contro le persone attraverso indagini e azioni penali efficaci, obbligo che risulta ancora più importante quando sia minacciato il benessere fisico e morale di un minore. Tuttavia, le misure che spetta alle autorità competenti adottare devono rispettare pienamente le regole del giusto procedimento e le altre garanzie idonee a limitare la portata dei poteri di indagine penale nonché gli altri diritti e libertà. In particolare, secondo detto giudice, occorre stabilire un quadro normativo che consenta di conciliare i diversi interessi e diritti da tutelare (Corte EDU, 28 ottobre 1998, Osman c. Regno Unito, CE:ECHR:1998:1028JUD002345294, §§ 115 e 116; 4 marzo 2004, M.C. c. Bulgaria, CE:ECHR:2003:1204JUD003927298, § 151; 24 giugno 2004, Von Hannover c. Germania, CE:ECHR:2004:0624JUD005932000, §§ 57 e 58, e 2 dicembre 2008, K.U. c. Finlandia, CE:ECHR:2008:1202JUD 000287202, §§ 46, 48 e 49).

129 Per quanto riguarda il rispetto del principio di proporzionalità, l'articolo 15, paragrafo 1, prima frase, della direttiva 2002/58 dispone che gli Stati membri possono adottare una misura che deroga al principio della riservatezza delle comunicazioni e dei dati relativi al traffico ad esse correlati qualora tale misura sia «necessaria, opportuna e proporzionata all'interno di una società democratica», alla luce degli obiettivi enunciati da detta disposizione. Il considerando 11 di detta direttiva precisa che una misura siffatta deve essere «strettamente» proporzionata allo scopo perseguito.

130 A tal riguardo, occorre ricordare che la tutela del diritto fondamentale al rispetto della vita privata esige, conformemente alla giurisprudenza costante della Corte, che le deroghe e le restrizioni alla tutela dei dati personali operino entro i limiti dello stretto necessario. Inoltre, un obiettivo di interesse generale non può essere perseguito senza tener conto del fatto che esso deve essere conciliato con i diritti fondamentali interessati dalla misura, effettuando un contemperamento equilibrato tra, da un lato, l'obiettivo di interesse generale e, dall'altro, i diritti di cui trattasi [v., in tal senso, sentenze del 16 dicembre 2008, Satakunnan Markkinapörssi e Satamedia, C-73/07, EU:C:2008:727, punto56; del 9 novembre 2010, Volker und Markus Schecke e Eifert, C-92/09 e C-93/09, EU:C:2010:662, punti 76, 77 e 86, e dell'8 aprile 2014, Digital Rights, C-293/12 e C-594/12, EU:C:2014:238, punto 52; parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, EU:C:2017:592, punto 140].

131 Più in particolare, dalla giurisprudenza della Corte risulta che la possibilità per gli Stati membri di giustificare una limitazione dei diritti e degli obblighi previsti, segnatamente, agli articoli 5, 6 e 9 della direttiva 2002/58 deve essere valutata misurando la gravità dell'ingerenza che una restrizione siffatta comporta e verificando che l'importanza dell'obiettivo di interesse generale perseguito da tale limitazione sia adeguata a detta gravità (v., in tal senso, sentenza del 2 ottobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punto 55 e giurisprudenza citata).

132 Per soddisfare il requisito di proporzionalità, una normativa deve prevedere norme chiare e precise che disciplinino la portata e l'applicazione della misura considerata e fissino un minimo di requisiti, di modo che le persone i cui dati personali sono oggetto di attenzione dispongano di garanzie sufficienti che consentano di proteggere efficacemente tali dati contro i rischi di abuso. Detta normativa deve essere giuridicamente vincolante nell'ambito dell'ordinamento nazionale e, in particolare, indicare in quali circostanze e a quali condizioni una misura che prevede il trattamento di siffatti dati possa essere adottata, garantendo così che l'ingerenza sia limitata allo stretto necessario. La necessità di disporre di siffatte garanzie è tanto più importante allorché i dati personali sono soggetti a trattamento automatizzato, in particolare quando esiste un rischio considerevole di accesso illecito ai dati stessi. Tali considerazioni valgono segnatamente quando è in gioco la protezione di quella categoria particolare di dati personali che sono i dati sensibili [v., in tal senso, sentenze dell'8 aprile 2014, Digital Rights, C-293/12 e C-594/12, EU:C:2014:238, punti 54 e 55, nonché del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punto 117; parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, EU:C:2017:592, punto 141].

133 Pertanto, una normativa che preveda una conservazione dei dati personali deve sempre rispondere a criteri oggettivi, che pongano un rapporto tra i dati personali da conservare e l'obiettivo perseguito [v., in tal senso, parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, EU:C:2017:592, punto 191 e giurisprudenza citata, nonché sentenza del 3 ottobre 2019, A e a., C-70/18, EU:C:2019:823, punto 63].

– Sulle misure legislative che prevedono la conservazione preventiva dei dati relativi al traffico e dei dati relativi all'ubicazione a fini di salvaguardia della sicurezza nazionale

134 Si deve osservare che l'obiettivo di salvaguardia della sicurezza nazionale, evocato dai giudici del rinvio e dai governi che hanno presentato osservazioni, non è ancora stato specificamente esaminato dalla Corte nelle sentenze che interpretano la direttiva 2002/58.

135 A tal riguardo, si deve anzitutto rilevare che l'articolo 4, paragrafo 2, TUE stabilisce che la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro. Detta competenza corrisponde all'interesse primario di tutelare le funzioni essenziali dello Stato e gli interessi fondamentali della società e comprende la prevenzione e la repressione di 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.

136 Orbene, l'importanza dell'obiettivo di salvaguardia della sicurezza nazionale, letto alla luce dell'articolo 4, paragrafo 2, TUE, 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. Infatti, minacce come quelle menzionate al punto precedente si distinguono, per la loro natura e la loro particolare gravità, dal rischio generale che si verifichino tensioni o perturbazioni, anche gravi, della pubblica sicurezza. 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.

137 Pertanto, in situazioni come quelle descritte ai punti 135 e 136 della presente sentenza, 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, non osta, in linea di principio, a una misura legislativa che autorizzi le autorità competenti ad imporre ai fornitori di servizi di comunicazione elettronica di procedere alla conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione di tutti gli utenti dei mezzi di comunicazione elettronica per un periodo limitato, se ricorrono circostanze sufficientemente concrete che consentono di ritenere che lo Stato membro interessato affronti una minaccia grave come quella indicata ai punti 135 e 136 della presente sentenza per la sicurezza nazionale che si rivela reale e attuale o prevedibile. Anche se una misura siffatta riguarda, in maniera indifferenziata, tutti gli utenti di mezzi di comunicazione elettronica senza che questi ultimi sembrino, a prima vista, presentare alcun collegamento, ai sensi della giurisprudenza richiamata al punto 133 della presente sentenza, con una minaccia per la sicurezza nazionale di tale Stato membro, si deve tuttavia considerare che l'esistenza di una simile minaccia è idonea, di per sé, a stabilire detto collegamento.

138 L'ingiunzione che prevede la conservazione preventiva dei dati di tutti gli utenti dei mezzi di comunicazione elettronica deve però essere temporalmente limitata allo stretto necessario. Se pure non può escludersi che l'ingiunzione che impone ai fornitori di servizi di comunicazione elettronica di procedere alla conservazione dei dati possa essere rinnovata, in ragione della persistenza di una minaccia di tal genere, la durata di ciascuna ingiunzione non può superare un lasso di tempo prevedibile. Inoltre, una siffatta conservazione dei dati deve essere soggetta a limitazioni ed accompagnarsi a garanzie rigorose che consentano di proteggere efficacemente i dati personali degli interessati contro il rischio di abusi. Pertanto, tale conservazione non può avere carattere sistematico.

139 Tenuto conto della gravità dell'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta risultante da una siffatta misura di conservazione generalizzata e indifferenziata dei dati, occorre garantire che il ricorso ad essa sia effettivamente limitato alle situazioni nelle quali sussiste una minaccia grave per la sicurezza nazionale, come quelle indicate ai punti 135 e 136 della presente sentenza. A tal fine, è essenziale che un provvedimento che impone ai fornitori di servizi di comunicazione elettronica di procedere a una siffatta conservazione dei dati possa essere oggetto 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 di una delle suddette situazioni nonché il rispetto delle condizioni e delle garanzie che devono essere previste.

– Sulle misure legislative che prevedono la conservazione preventiva dei dati relativi al traffico e dei dati relativi all'ubicazione a fini di lotta alla criminalità e di salvaguardia della sicurezza pubblica

140 Per quanto riguarda l'obiettivo di prevenzione, ricerca, accertamento e perseguimento dei reati, conformemente al principio di proporzionalità, solo la lotta alle forme gravi di criminalità e la prevenzione di 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 dei dati relativi al traffico e dei dati relativi all'ubicazione. Pertanto, solo le ingerenze in tali diritti fondamentali che non presentano un carattere grave possono essere giustificate dall'obiettivo di prevenzione, ricerca, accertamento e perseguimento di reati in generale [v., in tal senso, sentenze del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punto 102, e del 2 ottobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punti 56 e 57; parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, EU:C:2017:592, punto 149].

141 Una normativa nazionale che prevede la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione, ai fini della lotta alle forme gravi di criminalità, travalica i limiti dello stretto necessario e non può essere considerata giustificata, in una società democratica, così come richiede 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 (v., in tal senso, sentenza del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punto 107).

142 Infatti, tenuto conto del carattere sensibile delle informazioni che possono fornire i dati relativi al traffico e i dati relativi all'ubicazione, la riservatezza di tali dati è essenziale per il diritto al rispetto della vita privata. Pertanto, e tenuto conto, da un lato, degli effetti dissuasivi sull'esercizio dei diritti fondamentali sanciti dagli articoli 7 e 11 della Carta, menzionati al punto 118 della presente sentenza, che la conservazione di tali dati può determinare e, dall'altro, della gravità dell'ingerenza che una siffatta conservazione comporta, occorre, in una società democratica, che detta 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 una conservazione sistematica e continuativa. Questa conclusione si impone anche con riguardo agli obiettivi di lotta alle forme gravi di criminalità e di prevenzione delle minacce gravi alla sicurezza pubblica nonché all'importanza che occorre loro riconoscere.

143 Inoltre, la Corte ha sottolineato che una normativa che prevede la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione riguarda le comunicazioni elettroniche della quasi totalità della popolazione senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo perseguito. Una normativa siffatta, contrariamente al requisito ricordato al punto 133 della presente sentenza, riguarda in maniera globale l'insieme delle persone che fanno uso di mezzi di comunicazione elettronica, senza tuttavia che le persone i cui dati vengono conservati debbano trovarsi, anche indirettamente, in una situazione che possa dar luogo a indagini penali. Essa pertanto si applica anche a persone per le quali non esiste alcun indizio tale da far credere che il loro comportamento possa avere un nesso, ancorché indiretto o lontano, con reati gravi e, in particolare, senza che sia prevista una correlazione tra i dati di cui è prevista la conservazione e una minaccia per la sicurezza pubblica (v., in tal senso, sentenze dell'8 aprile 2014, Digital Rights, C-293/12 e C-594/12, EU:C:2014:238, punti 57 e 58, e del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punto 105).

144 In particolare, come già dichiarato dalla Corte, una normativa siffatta non limita la conservazione dei dati a quelli relativi a un determinato periodo di tempo e/o a un'area geografica determinata e/o a una cerchia di persone determinate che possano essere coinvolte, in un modo o nell'altro, in un reato grave, né alle persone la conservazione dei cui dati, per altri motivi, potrebbe contribuire alla lotta contro la criminalità grave (v., in tal senso, sentenze dell'8 aprile 2014, Digital Rights, C-293/12 e C-594/12, EU:C:2014:238, punto 59, e del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punto 106).

145 Orbene, anche gli obblighi positivi degli Stati membri che possono derivare, a seconda dei casi, dagli articoli 3, 4 e 7 della Carta e che riguardano, come rilevato ai punti 126 e 128 della presente sentenza, l'istituzione di norme che consentano una lotta effettiva contro i reati non possono avere l'effetto di giustificare ingerenze tanto gravi quanto quelle che comporta una normativa che prevede una conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta della quasi totalità della popolazione senza che i dati degli interessati siano idonei a rivelare una connessione, almeno indiretta, con l'obiettivo perseguito.

146 Per contro, conformemente a quanto rilevato ai punti da 142 a 144 della presente sentenza, e avuto riguardo al necessario contemperamento dei diritti e degli interessi in gioco, gli obiettivi di lotta alla criminalità grave, di prevenzione degli attentati gravi alla sicurezza pubblica e, a fortiori, di salvaguardia della sicurezza nazionale sono idonei a giustificare, tenuto conto della loro importanza, alla luce degli obblighi positivi ricordati al punto precedente e ai quali ha fatto riferimento in particolare la Cour constitutionnelle (Corte costituzionale), l'ingerenza particolarmente grave che comporta una conservazione mirata dei dati relativi al traffico e dei dati relativi all'ubicazione.

147 Pertanto, come già dichiarato dalla Corte, 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 la quale consenta, a titolo preventivo, una conservazione mirata dei dati relativi al traffico e dei dati relativi all'ubicazione, per finalità di lotta conto la criminalità grave e di

prevenzione delle minacce gravi alla sicurezza pubblica, nonché a fini di salvaguardia della sicurezza nazionale, a condizione che tale conservazione sia, per quanto concerne le categorie di dati da conservare, i mezzi di comunicazione interessati, le persone riguardate, nonché la durata di conservazione prevista, limitata allo stretto necessario (v., in tal senso, sentenza del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punto 108).

148 Per quanto riguarda i limiti cui deve essere soggetta una siffatta misura di conservazione dei dati, essi possono, in particolare, essere determinati in funzione delle categorie di persone interessate, in quanto l'articolo 15, paragrafo 1, della direttiva 2002/58 non osta a una normativa nazionale fondata su elementi oggettivi che permettano di prendere in considerazione le persone i cui dati relativi al traffico e all'ubicazione sono idonei a rivelare una connessione, almeno indiretta, con atti di criminalità grave, a contribuire in un modo o in un altro alla lotta contro la criminalità grave, o a prevenire un grave rischio per la sicurezza pubblica o, ancora, un rischio per la sicurezza nazionale (v., in tal senso, sentenza del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punto 111).

149 A tal riguardo, occorre precisare che le persone interessate possono essere in particolare quelle precedentemente identificate, nell'ambito delle procedure nazionali applicabili e sulla base di elementi oggettivi, come soggetti che costituiscono una minaccia per la sicurezza pubblica o la sicurezza nazionale dello Stato membro interessato.

150 La delimitazione di una misura che prevede la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione può essere fondata anche su un criterio geografico qualora le autorità nazionali competenti considerino, sulla base di elementi oggettivi e non discriminatori, che esiste, in una o più zone geografiche, una situazione caratterizzata da un rischio elevato di preparazione o di commissione di atti di criminalità grave (v., in tal senso, sentenza del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punto 111). 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 pedaggio.

151 Al fine di assicurare che l'ingerenza che comportano le misure di conservazione mirata descritte ai punti da 147 a 150 della presente sentenza sia conforme al principio di proporzionalità, la loro durata non può eccedere quella strettamente necessaria alla luce dell'obiettivo perseguito e delle circostanze che le giustificano, fatto salvo un eventuale rinnovo a motivo della persistenza della necessità di procedere a una siffatta conservazione.

– Sulle misure legislative che prevedono la conservazione preventiva degli indirizzi IP e dei dati relativi all'identità civile a fini di lotta alla criminalità e di salvaguardia della sicurezza pubblica

152 Occorre rilevare che gli indirizzi IP, pur facendo parte dei dati relativi al traffico, sono generati senza essere collegati a una comunicazione determinata e servono principalmente a identificare, tramite i fornitori di servizi di comunicazione elettronica, la persona fisica proprietaria di un'apparecchiatura terminale a partire dalla quale viene effettuata una comunicazione via Internet. Pertanto, in materia di posta elettronica e di telefonia via Internet, purché siano conservati solo gli indirizzi IP dell'origine della comunicazione e non quelli del destinatario della stessa, detti indirizzi non rivelano, in quanto tali, alcuna informazione sui terzi che sono stati in contatto con la persona all'origine della comunicazione. Questa categoria di dati presenta quindi un grado di sensibilità inferiore rispetto agli altri dati relativi al traffico.

153 Tuttavia, poiché gli indirizzi IP possono essere utilizzati per effettuare in particolare il tracciamento completo del percorso di navigazione di un utente di Internet e, di conseguenza, della sua attività online, tali dati consentono di stabilire il profilo dettagliato di quest'ultimo. Pertanto, la conservazione

e l'analisi di detti indirizzi IP necessari per un siffatto tracciamento costituiscono ingerenze gravi nei diritti fondamentali dell'utente di Internet sanciti dagli articoli 7 e 8 della Carta, che possono avere effetti dissuasivi come quelli indicati al punto 118 della presente sentenza.

154 Orbene, ai fini del necessario contemperamento dei diritti e degli interessi in gioco richiesto dalla giurisprudenza citata al punto 130 della presente sentenza, occorre tenere conto del fatto che, nel caso di un reato commesso online, l'indirizzo IP può costituire l'unico strumento di indagine che permetta di identificare la persona alla quale tale indirizzo era attribuito al momento della commissione di detto reato. A ciò si aggiunge il fatto che la conservazione degli indirizzi IP da parte dei fornitori di servizi di comunicazione elettronica oltre la durata dell'attribuzione di tali dati non appare necessaria, in linea di principio, ai fini della fatturazione dei servizi di cui trattasi, di modo che l'accertamento dei reati commessi online può, per questo motivo, come hanno indicato vari governi nelle loro osservazioni presentate alla Corte, rivelarsi impossibile senza ricorrere a una misura legislativa ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58. Ciò può valere in particolare, come sostenuto da detti governi, per i reati particolarmente gravi in materia di pornografia minorile, quali l'acquisto, la diffusione, la trasmissione o la messa a disposizione online di materiale pedopornografico, ai sensi dell'articolo 2, lettera c), della direttiva 2011/93/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio (GU 2011, L 335, pag. 1).

155 Ciò posto, se pure è vero che una misura legislativa che prevede la conservazione degli indirizzi IP di tutte le persone fisiche proprietarie di un'apparecchiatura terminale a partire dalla quale può essere effettuato un accesso a Internet riguarderebbe persone che, a prima vista, non presentano un collegamento, ai sensi della giurisprudenza citata al punto 133 della presente sentenza, con gli obiettivi perseguiti, e che gli utenti di Internet dispongono, conformemente a quanto osservato supra al punto 109, del diritto di attendersi, in forza degli articoli 7 e 8 della Carta, che la loro identità, in linea di principio, non sia rivelata, una misura legislativa che preveda la conservazione generalizzata e indifferenziata dei soli indirizzi IP attribuiti all'origine di una connessione non risulta, in linea di principio, contraria all'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, purché tale possibilità sia subordinata al rigoroso rispetto delle condizioni sostanziali e procedurali che devono disciplinare l'utilizzo dei dati in questione.

156 Tenuto conto della gravità dell'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta che tale conservazione comporta, 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.

157 Per quanto concerne, infine, i dati relativi all'identità civile degli utenti dei mezzi di comunicazione elettronica, tali dati non consentono, di per sé, 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 di esse con talune persone nel corso di un determinato periodo, cosicché non forniscono, a parte le coordinate di queste ultime, quali i loro indirizzi, alcuna informazione sulle comunicazioni dati e, di conseguenza, sulla loro vita privata. Pertanto, l'ingerenza che comporta una conservazione di tali dati non può, in linea di principio, essere qualificata come grave (v., in tal senso, sentenza del 2 ottobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punti 59 e 60).

158 Ne consegue che, conformemente a quanto esposto al punto 140 della presente sentenza, le misure legislative riguardanti il trattamento dei suddetti dati in quanto tali, in particolare la loro conservazione e l'accesso agli stessi al solo scopo di identificare l'utente interessato, e senza che tali

dati possano essere associati ad informazioni relative alle comunicazioni effettuate, possono essere giustificate dall'obiettivo di prevenzione, ricerca, accertamento e perseguimento di reati in generale, di cui all'articolo 15, paragrafo 1, prima frase, della direttiva 2002/58 (v., in tal senso, sentenza del 2 ottobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punto 62).

159 Ciò posto, tenuto conto del necessario contemperamento dei diritti e degli interessi in gioco e per i motivi illustrati supra ai punti 131 e 158, si deve ritenere che, anche in assenza di un nesso tra tutti gli utenti dei mezzi di comunicazione elettronica e gli obiettivi perseguiti, 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, non osti a una misura legislativa che imponga, senza un termine particolare, ai fornitori di servizi di comunicazione elettronica di conservare i dati relativi all'identità civile di tutti gli utenti di mezzi di comunicazione elettronica a fini di prevenzione, ricerca, accertamento e perseguimento dei reati nonché di salvaguardia della sicurezza pubblica, senza che sia necessario che i reati oppure le minacce o gli attentati alla sicurezza pubblica siano gravi.

– Sulle misure legislative che prevedono la conservazione rapida dei dati relativi al traffico e dei dati relativi all'ubicazione a fini di lotta alle forme gravi di criminalità

160 Per quanto riguarda i dati relativi al traffico e i dati relativi all'ubicazione trattati e memorizzati dai fornitori di servizi di comunicazione elettronica sulla base degli articoli 5, 6 e 9 della direttiva 2002/58, o sulla base di misure legislative adottate in forza dell'articolo 15, paragrafo 1, della stessa, quali descritte ai punti da 134 a 159 della presente sentenza, si deve rilevare che tali dati, in linea di principio, devono essere, a seconda dei casi, cancellati o resi anonimi alla scadenza dei termini legali entro i quali devono avvenire, conformemente alle disposizioni nazionali che recepiscono detta direttiva, il loro trattamento e la loro memorizzazione.

161 Tuttavia, durante il trattamento o la memorizzazione possono presentarsi situazioni nelle quali si pone l'esigenza di conservare i dati in questione oltre i suddetti termini al fine di indagare su reati gravi o attentati alla sicurezza nazionale, e ciò sia quando tali reati o attentati abbiano già potuto essere constatati, sia quando la loro esistenza possa essere ragionevolmente sospettata in esito ad un esame obiettivo di tutte le circostanze pertinenti.

162 A tal riguardo, occorre rilevare che la Convenzione sulla criminalità informatica del Consiglio d'Europa, del 23 novembre 2001 (serie dei trattati europei n. 185), che è stata sottoscritta dai 27 Stati membri e ratificata da 25 di essi, e il cui obiettivo è facilitare la lotta contro i reati commessi mediante reti informatiche, prevede, all'articolo 14, che le parti contraenti adottano per indagini o procedimenti penali specifici determinate misure riguardo ai dati relativi al traffico già memorizzati, quale la conservazione rapida di tali dati. In particolare, l'articolo 16, paragrafo 1, di detta convenzione stabilisce che le parti contraenti adottano le misure legislative necessarie per consentire alle loro autorità competenti di ordinare o ottenere in altro modo la conservazione rapida dei dati relativi al traffico memorizzati attraverso un sistema informatico, soprattutto quando vi è motivo di ritenere che tali dati siano esposti a perdita o alterazione.

163 In una situazione come quella indicata al punto 161 della presente sentenza, gli Stati membri, tenuto conto del necessario contemperamento dei diritti e degli interessi in gioco indicato supra al punto 130, possono prevedere, in una normativa adottata sulla base dell'articolo 15, paragrafo 1, della direttiva 2002/58, la possibilità di ordinare ai fornitori di comunicazione elettronica, mediante un provvedimento dell'autorità competente soggetto 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 dei quali dispongono.

164 Dato che la finalità di una siffatta conservazione rapida non corrisponde più a quelle per le quali i dati sono stati raccolti e conservati inizialmente e poiché qualsiasi trattamento di dati deve, ai sensi dell'articolo 8, paragrafo 2, della Carta, rispondere a finalità determinate, gli Stati membri devono precisare, nella loro legislazione, il fine per il quale può aver luogo la conservazione rapida dei dati. Tenuto conto della gravità dell'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta che una siffatta conservazione può comportare, solo la lotta alle forme gravi di criminalità e, a fortiori, la salvaguardia della sicurezza nazionale sono idonee a giustificare tale ingerenza. Inoltre, al fine di garantire che l'ingerenza che una misura di questo tipo comporta sia limitata allo stretto necessario, occorre, da un lato, che l'obbligo di conservazione riguardi unicamente i dati relativi al traffico e i dati relativi all'ubicazione che possono contribuire all'accertamento del reato grave o dell'attentato alla sicurezza nazionale di cui trattasi. Dall'altro, la durata di conservazione dei dati deve essere limitata allo stretto necessario, potendo tuttavia essere prorogata quando le circostanze e l'obiettivo perseguito da detta misura lo giustifichino.

165 A tal riguardo, occorre precisare che una siffatta conservazione rapida non deve essere limitata ai dati delle persone concretamente sospettate di avere commesso un reato o un attentato alla sicurezza nazionale. Pur rispettando il quadro delineato dall'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, e tenuto conto delle considerazioni esposte supra al punto 133, una misura del genere può, a scelta del legislatore e nel rispetto dei limiti dello stretto necessario, essere estesa ai dati relativi al traffico e ai dati relativi all'ubicazione afferenti 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, del suo ambiente sociale o professionale o ancora di zone geografiche determinate, quali i luoghi della commissione e della preparazione del reato o dell'attentato alla sicurezza nazionale di cui trattasi. Inoltre, l'accesso delle autorità competenti ai dati in tal modo conservati deve essere effettuato nel rispetto delle condizioni risultanti dalla giurisprudenza che ha interpretato la direttiva 2002/58 (v., in tal senso, sentenza del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punti da 118 a 121 e giurisprudenza citata).

166 Occorre ancora aggiungere che, come risulta in particolare dai punti 115 e 133 della presente sentenza, l'accesso ai dati relativi al traffico e ai dati relativi all'ubicazione conservati da fornitori in applicazione di una misura adottata ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58 può, in linea di principio, essere giustificato unicamente dall'obiettivo di interesse generale per il quale siffatta conservazione è stata imposta a detti fornitori. Ne consegue, in particolare, che l'accesso ai dati di cui trattasi a fini di repressione e sanzione di un reato comune non può essere accordato in alcun caso qualora la loro conservazione sia stata giustificata dall'obiettivo di lotta alla criminalità grave o, a fortiori, di salvaguardia della sicurezza nazionale. Per contro, conformemente al principio di proporzionalità quale precisato al punto 131 della presente sentenza, l'accesso a dati conservati ai fini della lotta alla criminalità grave può essere giustificato dall'obiettivo di salvaguardia della sicurezza nazionale, purché siano rispettate le condizioni sostanziali e procedurali relative a detto accesso indicate al punto precedente.

167 A tal riguardo, agli Stati membri è data facoltà di prevedere nella loro legislazione che l'accesso ai dati relativi al traffico e ai dati relativi all'ubicazione possa avere luogo, nel rispetto di queste stesse condizioni sostanziali e procedurali, a fini di lotta alla criminalità grave o di salvaguardia della sicurezza nazionale, quando i suddetti dati siano conservati da un fornitore in modo conforme agli articoli 5, 6 e 9 o all'articolo 15, paragrafo 1, della direttiva 2002/58.

168 Alla luce di tutte le considerazioni che precedono, occorre rispondere alle prime questioni nelle cause C-511/18 e C-512/18 nonché alle questioni prima e seconda nella causa C-520/18 dichiarando che 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, deve essere interpretato nel senso che osta a misure legislative che prevedono, ai fini di cui all'articolo 15, paragrafo 1, a titolo preventivo, una

conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione. Per contro, l'articolo 15, paragrafo 1, letto alla luce degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta, non osta a misure legislative

– che consentano, a fini di salvaguardia della sicurezza nazionale, il 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, e 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;

– che prevedano, a fini di salvaguardia della sicurezza nazionale, di lotta alle forme gravi di criminalità e di prevenzione delle minacce gravi alla sicurezza pubblica, una 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;

– che prevedano, a fini di salvaguardia della sicurezza nazionale, di lotta alle forme gravi di criminalità e di prevenzione delle minacce gravi alla sicurezza pubblica, la conservazione generalizzata e indifferenziata degli indirizzi IP attribuiti all'origine di una connessione, per un periodo temporalmente limitato allo stretto necessario;

– che prevedano, a fini di salvaguardia della sicurezza nazionale, di lotta alla criminalità e di salvaguardia della sicurezza pubblica, una conservazione generalizzata e indifferenziata dei dati relativi all'identità civile degli utenti di mezzi di comunicazione elettronica, e

– che consentano, a fini di lotta alle forme gravi di criminalità e, a fortiori, di salvaguardia della sicurezza nazionale, il ricorso a un'ingiunzione che imponga ai fornitori di servizi di comunicazione elettronica, mediante un provvedimento dell'autorità competente soggetto 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 detti fornitori di servizi dispongono,

se tali misure garantiscono, 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.

Sulle questioni seconda e terza nella causa C-511/18

169 Con la seconda e la terza questione nella causa C-511/18, il giudice del rinvio chiede, in sostanza, 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 a 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 nonché la raccolta in tempo reale dei dati relativi al traffico e dei dati 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 raccolte.

170 Il giudice del rinvio precisa che le tecniche di raccolta di informazioni di cui agli articoli da L. 851-2 a L. 851-4 del CSI non implicano, per i fornitori di servizi di comunicazione elettronica, un obbligo specifico di conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione. Per quanto riguarda, in particolare, l'analisi automatizzata di cui all'articolo L. 851-3 del CSI, tale giudice rileva che siffatto trattamento ha lo scopo di individuare, in funzione di criteri all'uopo definiti, connessioni in grado di rivelare una minaccia terroristica. Quanto alla raccolta in tempo reale di cui all'articolo L. 851-2 del CSI, detto giudice constata che essa riguarda unicamente una o più persone precedentemente identificate come potenzialmente collegate a una minaccia terroristica. Secondo il medesimo giudice, queste due tecniche possono essere attuate solo a fini di prevenzione del terrorismo e hanno ad oggetto i dati menzionati agli articoli L. 851-1 e R. 851-5 del CSI.

171 In via preliminare, occorre precisare che la circostanza che, ai sensi dell'articolo L. 851-3 del CSI, l'analisi automatizzata da esso prevista non consenta, di per sé, l'identificazione degli utenti i cui dati sono sottoposti a siffatta analisi non osta alla qualificazione di tali dati come «dati personali». Infatti, dal momento che la procedura prevista al paragrafo IV della medesima disposizione consente, in una fase successiva, l'identificazione della persona o delle persone interessate dai dati la cui analisi automatizzata ha rivelato la loro idoneità a qualificare l'esistenza di una minaccia terroristica, tutte le persone i cui dati formano oggetto dell'analisi automatizzata sono identificabili a partire da detti dati. Orbene, secondo la definizione dei dati personali contenuta nell'articolo 4, punto 1, del regolamento 2016/679, costituiscono tali dati le informazioni riguardanti, in particolare, una persona identificabile.

Sull'analisi automatizzata dei dati relativi al traffico e dei dati relativi all'ubicazione

172 Dall'articolo L. 851-3 del CSI risulta che l'analisi automatizzata da esso prevista corrisponde, in sostanza, a 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. Ne consegue che i dati degli utenti dei mezzi di comunicazione elettronica sono tutti verificati se corrispondono a tali parametri. Pertanto, si deve ritenere che una siffatta analisi automatizzata implichi, per i fornitori di servizi di comunicazione elettronica interessati, l'attuazione, per conto dell'autorità competente, di un trattamento generalizzato e indifferenziato, sotto forma di utilizzo con l'ausilio di un processo automatizzato, ai sensi dell'articolo 4, punto 2, del regolamento 2016/679, che copre l'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione di tutti gli utenti di mezzi di comunicazione elettronica. Detto trattamento è indipendente dalla raccolta successiva dei dati relativi alle persone identificate a seguito dell'analisi automatizzata, raccolta che è autorizzata sul fondamento dell'articolo L. 851-3, paragrafo IV, del CSI.

173 Orbene, una normativa nazionale che autorizza una siffatta analisi automatizzata dei dati relativi al traffico e dei dati relativi all'ubicazione deroga all'obbligo di principio, posto all'articolo 5 della direttiva 2002/58, di garantire la riservatezza delle comunicazioni elettroniche e dei dati a queste correlati. Una siffatta normativa costituisce inoltre un'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta, indipendentemente dall'uso ulteriore di tali dati. Infine, conformemente alla giurisprudenza citata al punto 118 della presente sentenza, detta normativa può produrre effetti dissuasivi sull'esercizio della libertà di espressione sancita dall'articolo 11 della Carta.

174 Inoltre, l'ingerenza risultante da un'analisi automatizzata dei dati relativi al traffico e dei dati relativi all'ubicazione, come quella di cui trattasi nei procedimenti principali, appare particolarmente grave in quanto riguarda in modo generalizzato e indifferenziato i dati delle persone che si avvalgono dei mezzi di comunicazione elettronica. Tale constatazione si impone a maggior ragione quando, come risulta dalla normativa nazionale di cui trattasi nei procedimenti principali, i dati oggetto dell'analisi automatizzata sono idonei a rivelare la natura delle informazioni consultate online. Oltre a ciò, una siffatta analisi automatizzata si applica globalmente a tutte le persone che si avvalgono di mezzi di

comunicazione elettronica e, di conseguenza, anche a quelle per le quali non esiste alcun indizio tale da indurre a ritenere che il loro comportamento possa presentare un nesso, sia pur indiretto o remoto, con attività terroristiche.

175 Per quanto riguarda la giustificazione di tale ingerenza, occorre precisare che il requisito, posto all'articolo 52, paragrafo 1, della Carta, secondo cui qualsiasi limitazione nell'esercizio dei diritti fondamentali deve essere prevista dalla legge implica che la base giuridica che consente l'ingerenza in tali diritti deve definire essa stessa la portata della limitazione dell'esercizio del diritto considerato (v., in tal senso, sentenza del 16 luglio 2020, Facebook Ireland e Schrems, C-311/18, EU:C:2020:559, punto 175 e giurisprudenza citata).

176 Inoltre, per soddisfare il requisito di proporzionalità ricordato ai punti 130 e 131 della presente sentenza, secondo cui le deroghe e le restrizioni alla protezione dei dati personali devono operare entro i limiti dello stretto necessario, una normativa nazionale che disciplina l'accesso delle autorità competenti a dati relativi al traffico e a dati relativi all'ubicazione conservati deve rispettare i requisiti risultanti dalla giurisprudenza citata supra al punto 132. In particolare, una siffatta normativa non può limitarsi ad esigere che l'accesso a detti dati risponda ad una delle finalità perseguite da detta normativa, ma deve prevedere anche le condizioni sostanziali e procedurali che disciplinino tale uso [v., in tal senso, parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, EU:C:2017:592, punto 192 e giurisprudenza citata].

177 A tal riguardo, occorre ricordare che l'ingerenza particolarmente grave che comporta una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione, oggetto delle considerazioni esposte ai punti da 134 a 139 della presente sentenza, nonché l'ingerenza particolarmente grave costituita dalla loro analisi automatizzata possono soddisfare il requisito di proporzionalità solo in situazioni nelle quali uno Stato membro si trovi di fronte ad una minaccia grave per la sicurezza nazionale che risulti reale e attuale o prevedibile, e a condizione che la durata di tale conservazione sia limitata allo stretto necessario.

178 In situazioni come quelle indicate al punto precedente, l'attuazione di un'analisi automatizzata dei dati relativi al traffico e dei dati relativi all'ubicazione di tutti gli utenti di mezzi di comunicazione elettronica, per un periodo strettamente limitato, può essere considerata 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.

179 Ciò premesso, al fine di garantire che il ricorso a una siffatta misura sia effettivamente limitato a quanto strettamente necessario per la salvaguardia della sicurezza nazionale, e più in particolare per la prevenzione del terrorismo, è essenziale, conformemente a quanto constatato al punto 139 della presente sentenza, che il provvedimento che autorizza l'analisi automatizzata 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 a verificare l'esistenza di una situazione che giustifichi detto provvedimento e il rispetto delle garanzie che devono essere previste.

180 A tal riguardo, occorre precisare che i modelli e i criteri prestabiliti sui quali si fonda tale tipo di trattamento di dati devono essere, da un lato, specifici e affidabili, consentendo di raggiungere risultati che identifichino gli individui sui quali potrebbe gravare un sospetto ragionevole di partecipazione a reati di terrorismo e, dall'altro, non discriminatori [v., in tal senso, parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, EU:C:2017:592, punto 172].

181 Inoltre, si deve ricordare che qualsiasi analisi automatizzata effettuata in funzione di modelli e criteri fondati sul postulato secondo cui l'origine etnica o razziale, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, la salute o l'orientamento sessuale di una persona potrebbero, di per se stesse e indipendentemente dal comportamento individuale di tale persona, essere rilevanti rispetto alla prevenzione del terrorismo violerebbe i diritti garantiti agli articoli 7 e 8

della Carta, letti in combinato disposto con l'articolo 21 della stessa. Pertanto, i modelli e i criteri prestabiliti ai fini di un'analisi automatizzata volta a prevenire attività di terrorismo che rappresentano una grave minaccia per la sicurezza nazionale non possono essere fondati solo su tali dati sensibili [v., in tal senso, parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, EU:C:2017:592, punto 165].

182 Inoltre, dal momento che le analisi automatizzate dei dati relativi al traffico e dei dati relativi all'ubicazione comportano necessariamente un certo tasso di errore, qualsiasi risultato positivo ottenuto a seguito di un trattamento automatizzato deve essere sottoposto a un riesame individuale con strumenti non automatizzati prima dell'adozione di una misura individuale che produca effetti pregiudizievoli nei confronti delle persone interessate, quale la raccolta successiva dei dati relativi al traffico e dei dati ubicazione in tempo reale; una misura siffatta non può infatti essere fondata in modo determinante soltanto sul risultato di un trattamento automatizzato. Analogamente, per garantire, in pratica, che i modelli e i criteri prestabiliti, l'uso che ne viene fatto nonché le banche dati utilizzate non abbiano natura discriminatoria e siano limitati allo stretto necessario rispetto all'obiettivo di prevenire attività di terrorismo che rappresentano una minaccia grave per la sicurezza nazionale, l'affidabilità e l'aggiornamento di tali modelli e criteri prestabiliti nonché delle banche dati utilizzate devono essere oggetto di un regolare riesame [v., in tal senso, parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, EU:C:2017:592, punti 173 e 174].

Sulla raccolta in tempo reale dei dati relativi al traffico e dei dati relativi all'ubicazione

183 Per quanto riguarda la raccolta in tempo reale dei dati relativi al traffico e dei dati relativi all'ubicazione prevista all'articolo L. 851-2 del CSI, si deve rilevare che essa può essere individualmente autorizzata in relazione a «una persona precedentemente identificata come potenzialmente collegata a una minaccia [terroristica]». Inoltre, secondo tale disposizione, «[q]ualora 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».

184 I dati che costituiscono l'oggetto di una misura di questa natura consentono alle autorità nazionali competenti di sorvegliare, per la durata dell'autorizzazione, in modo continuativo e in tempo reale, gli interlocutori con i quali le persone interessate comunicano, i mezzi da queste utilizzati, la durata delle loro comunicazioni nonché i loro luoghi di soggiorno e i loro spostamenti. Sembra inoltre che possano rivelare la natura delle informazioni consultate online. Presi nel loro insieme, tali dati sono idonei a consentire, come risulta dal punto 117 della presente sentenza, di trarre conclusioni molto precise riguardo alla vita privata delle persone interessate e forniscono gli strumenti per stabilire il profilo di dette persone, informazione altrettanto sensibile, in rapporto al diritto al rispetto della vita privata, quanto il contenuto stesso delle comunicazioni.

185 Per quel che riguarda la raccolta di dati in tempo reale prevista all'articolo L. 851-4 del CSI, detta disposizione autorizza la raccolta dei dati tecnici relativi all'ubicazione delle apparecchiature terminali e la trasmissione in tempo reale a un servizio del Primo ministro. Risulta che tali dati consentono al servizio competente, in qualsiasi momento per la durata dell'autorizzazione, di localizzare, in maniera continuativa e in tempo reale, le apparecchiature terminali utilizzate, quali telefoni cellulari.

186 Orbene, una normativa nazionale che autorizza siffatte raccolte in tempo reale deroga, al pari di quella che autorizza l'analisi automatizzata dei dati, all'obbligo di principio, posto all'articolo 5 della direttiva 2002/58, di garantire la riservatezza delle comunicazioni elettroniche e dei dati a queste correlati. Essa costituisce pertanto anche un'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta e può comportare effetti dissuasivi sull'esercizio della libertà di espressione garantita dall'articolo 11 della Carta.

187 Occorre sottolineare che l'ingerenza derivante dalla raccolta in tempo reale dei dati che consentono di localizzare un'apparecchiatura terminale risulta particolarmente grave, dato che tali dati forniscono alle autorità nazionali competenti uno strumento di controllo preciso e permanente degli spostamenti degli utenti dei telefoni mobili. Poiché questi dati devono quindi essere considerati particolarmente sensibili, l'accesso in tempo reale delle autorità competenti a siffatti dati deve essere tenuto distinto da un accesso in tempo differito agli stessi, essendo il primo più intrusivo in quanto consente una sorveglianza quasi totale di detti utenti (v., per analogia, relativamente all'articolo 8 della CEDU, Corte EDU, 8 febbraio 2018, Ben Faiza c. Francia, CE:ECHR:2018:0208JUD003144612, § 74). L'intensità di tale ingerenza è inoltre aggravata quando la raccolta in tempo reale si estende anche ai dati relativi al traffico delle persone interessate.

188 Sebbene l'obiettivo di prevenzione del terrorismo perseguito dalla normativa nazionale di cui trattasi nei procedimenti principali sia idonea, considerata la sua importanza, a giustificare l'ingerenza che comporta la raccolta in tempo reale dei dati relativi al traffico e dei dati relativi all'ubicazione, una misura siffatta può essere attuata, tenuto conto del suo carattere particolarmente intrusivo, solo nei confronti delle persone rispetto alle quali esiste un valido motivo per sospettare che esse siano implicate, in un modo o nell'altro, in attività di terrorismo. Quanto ai dati delle persone che non rientrano in tale categoria, essi possono essere oggetto soltanto di un accesso in tempo differito, che può avere luogo, conformemente alla giurisprudenza della Corte, solo in situazioni particolari, come quelle riguardanti 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 (v., in tal senso, sentenza del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punto 119 e giurisprudenza citata).

189 Inoltre, un provvedimento che autorizza la raccolta in tempo reale dei dati relativi al traffico e dei dati relativi all'ubicazione deve essere fondato su criteri oggettivi previsti dalla legislazione nazionale. In particolare, tale legislazione deve definire, conformemente alla giurisprudenza citata al punto 176 della presente sentenza, le circostanze e le condizioni in presenza delle quali una raccolta siffatta può essere autorizzata e prevedere che, come precisato al punto precedente, possano essere interessate unicamente le persone che presentano un collegamento con l'obiettivo di prevenzione del terrorismo. Inoltre, un provvedimento che autorizza la raccolta in tempo reale dei dati relativi al traffico e dei dati relativi all'ubicazione deve essere fondato su criteri oggettivi e non discriminatori previsti dalla legislazione nazionale. Al fine di garantire, in pratica, il rispetto di tali condizioni, è essenziale che l'attuazione del provvedimento che autorizza la raccolta in tempo reale sia subordinata ad un controllo preventivo effettuato da un giudice o da un organo amministrativo indipendente, la cui decisione sia dotata di effetto vincolante, e detto giudice o organo deve accertarsi, tra l'altro, che tale raccolta in tempo reale sia autorizzata solo nei limiti di quanto strettamente necessario (v., in tal senso, sentenza del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punto 120). In caso di emergenza debitamente giustificata, il controllo deve avvenire tempestivamente.

Sull'informazione delle persone i cui dati sono stati raccolti o analizzati

190 Le autorità nazionali competenti che procedono alla raccolta in tempo reale dei dati relativi al traffico e dei dati relativi all'ubicazione devono informarne le persone interessate, nell'ambito delle procedure nazionali applicabili, purché e a partire dal momento in cui tale comunicazione non possa compromettere le funzioni di dette autorità. Infatti, questa informazione è, de facto, necessaria per consentire a dette persone di esercitare i loro diritti, derivanti dagli articoli 7 e 8 della Carta, di chiedere l'accesso ai propri dati personali costituenti l'oggetto di tali misure e, se del caso, la rettifica o la cancellazione degli stessi, nonché di proporre, conformemente all'articolo 47, primo comma, della Carta, un ricorso effettivo dinanzi a un giudice, diritto peraltro espressamente garantito dall'articolo 15, paragrafo 2, della direttiva 2002/58, letto in combinato disposto con l'articolo 79, paragrafo 1, del

regolamento 2016/679 [v., in tal senso, sentenza del 21 dicembre 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, punto 121 e giurisprudenza citata, nonché parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, EU:C:2017:592, punti 219 e 220].

191 Per quanto riguarda l'informazione richiesta nel contesto di un'analisi automatizzata dei dati relativi al traffico e dei dati relativi all'ubicazione, l'autorità nazionale competente è tenuta a pubblicare informazioni di natura generale relative a tale analisi, senza dover informare individualmente le persone interessate. Per contro, nell'ipotesi in cui i dati rispondano ai parametri precisati nel provvedimento che autorizza l'analisi automatizzata e la menzionata autorità proceda all'identificazione della persona interessata al fine di analizzare più approfonditamente i dati che la riguardano, l'informazione individuale di tale persona risulta necessaria. Tuttavia, una siffatta informazione deve avvenire soltanto a partire dal momento in cui essa non può compromettere le funzioni di detta autorità [v., per analogia, parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, EU:C:2017:592, punti da 222 a 224].

192 Alla luce di tutte le considerazioni che precedono, occorre rispondere alle questioni seconda e terza nella causa C-511/18 dichiarando che 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, deve essere interpretato nel senso che non osta a una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica di ricorrere, da un lato, all'analisi automatizzata nonché alla raccolta in tempo reale, in particolare, dei dati relativi al traffico e dei dati relativi all'ubicazione e, dall'altro, alla raccolta in tempo reale dei dati tecnici relativi all'ubicazione delle apparecchiature terminali utilizzate, quando

– il ricorso all'analisi automatizzata è limitato a situazioni nelle quali uno Stato membro si trova ad affrontare una minaccia grave per la sicurezza nazionale che si rivela reale e attuale o prevedibile e il ricorso a tale analisi può essere oggetto di un controllo effettivo, da parte di un giudice o di un organo amministrativo indipendente, la cui decisione è dotata di effetto vincolante, diretto a verificare l'esistenza di una situazione idonea a giustificare detta misura nonché il rispetto delle condizioni e delle garanzie che devono essere previste, e quando

– il ricorso a una raccolta in tempo reale dei dati relativi al traffico e dei dati relativi all'ubicazione è limitato alle persone nei confronti delle quali esiste un valido motivo per sospettare che esse siano implicate, in un modo o nell'altro, in attività di terrorismo ed è soggetto a un controllo preventivo, effettuato da un giudice o da un organo amministrativo indipendente, la cui decisione ha effetto vincolante, al fine di accertarsi che tale raccolta in tempo reale sia autorizzata soltanto nei limiti di quanto strettamente necessario. In caso di emergenza debitamente giustificata, il controllo deve avvenire tempestivamente.

Sulla seconda questione nella causa C-512/18

193 Con la seconda questione nella causa C-512/18, il giudice del rinvio chiede, in sostanza, se le disposizioni della direttiva 2000/31, 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 a 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.

194 Pur considerando che siffatti servizi rientrano nell'ambito di applicazione della direttiva 2000/31, e non in quello della direttiva 2002/58, il giudice del rinvio è dell'avviso che l'articolo 15, paragrafi 1 e 2, della direttiva 2000/31, letto in combinato disposto con gli articoli 12 e 14 della stessa, non introduca, di per sé, un divieto di principio di conservare dati relativi alla creazione di contenuto al quale possa

derogarsi solo in via eccezionale. Detto giudice si chiede tuttavia se tale valutazione debba essere applicata, tenuto conto della necessità di rispettare i diritti fondamentali sanciti dagli articoli da 6 a 8 e 11 della Carta.

195 Inoltre, il giudice del rinvio precisa che la sua questione riguarda l'obbligo di conservazione previsto all'articolo 6 della LCEN, letto in combinato disposto con il decreto n. 2011-219. I dati che i fornitori di servizi interessati devono conservare a tale titolo comprendono, in particolare, i dati relativi all'identità civile delle persone che si sono avvalse di detti servizi, quali nome e cognome, gli indirizzi postali associati, gli indirizzi di posta elettronica o di account associati, le password e, qualora la sottoscrizione del contratto o dell'account sia a pagamento, il tipo di pagamento utilizzato, il riferimento del pagamento, l'importo nonché la data e l'ora dell'operazione.

196 Inoltre, i dati oggetto dell'obbligo di conservazione includono gli identificativi degli abbonati, delle connessioni e delle apparecchiature terminali utilizzate, gli identificativi attribuiti ai contenuti, la data e l'ora di inizio e di fine delle connessioni e delle operazioni nonché i tipi di protocolli utilizzati per la connessione al servizio e il trasferimento dei contenuti. L'accesso a tali dati, che sono conservati per un periodo di un anno, può essere richiesto nell'ambito di procedimenti penali e civili, al fine di far rispettare le norme relative alla responsabilità civile o penale, nonché nell'ambito di misure di raccolta di informazioni alle quali si applica l'articolo L. 851-1 del CSI.

197 A tal riguardo, occorre rilevare che, conformemente al suo articolo 1, paragrafo 2, la direttiva 2000/31 ravvicina talune disposizioni nazionali applicabili ai servizi della società dell'informazione di cui al suo articolo 2, lettera a).

198 È vero che tali servizi comprendono quelli prestati a distanza mediante attrezzature elettroniche di trattamento e di memorizzazione di dati, a richiesta individuale di un destinatario di servizi e, normalmente, dietro retribuzione, quali servizi di accesso a Internet o a una rete di comunicazione e servizi di hosting (v., in tal senso, sentenze del 24 novembre 2011, Scarlet Extended, C-70/10, EU:C:2011:771, punto 40; del 16 febbraio 2012, SABAM, C-360/10, EU:C:2012:85, punto 34; del 15 settembre 2016, Mc Fadden, C-484/14, EU:C:2016:689, punto 55, e del 7 agosto 2018, SNB-REACT, C-521/17, EU:C:2018:639, punto 42 e giurisprudenza citata).

199 Tuttavia, l'articolo 1, paragrafo 5, della direttiva 2000/31 dispone che quest'ultima non si applica alle questioni relative ai servizi della società dell'informazione oggetto delle direttive 95/46 e 97/66. A tal riguardo, dai considerando 14 e 15 della direttiva 2000/31 risulta che la tutela della riservatezza delle comunicazioni e delle persone fisiche con riguardo al trattamento dei dati personali nell'ambito dei servizi della società dell'informazione è disciplinata unicamente dalle direttive 95/46 e 97/66 e quest'ultima vieta, all'articolo 5, a fini di tutela della riservatezza delle comunicazioni, qualsiasi forma di intercettazione o di sorveglianza delle comunicazioni.

200 Pertanto, 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, che hanno sostituito rispettivamente la direttiva 97/66 e la direttiva 95/46, fermo restando che la tutela che la direttiva 2000/31 mira a garantire non può comunque violare le prescrizioni della direttiva 2002/58 e del regolamento 2016/679 (v., in tal senso, sentenza del 29 gennaio 2008, Promusicae, C-275/06, EU:C:2008:54, punto 57).

201 L'obbligo imposto dalla normativa nazionale menzionata al punto 195 della presente sentenza ai fornitori di accesso a servizi di comunicazione al pubblico online e ai fornitori di servizi di hosting di conservare dati personali relativi a tali servizi deve quindi essere valutato, come ha rilevato in sostanza l'avvocato generale al paragrafo 141 delle conclusioni nelle cause riunite La Quadrature du Net e a. (C-511/18 e C-512/18, EU:C:2020:6), alla luce della direttiva 2002/58 o del regolamento 2016/679.

202 Pertanto, a seconda che rientri o meno nell'ambito di applicazione della direttiva 2002/58, la fornitura dei servizi coperti da tale normativa nazionale sarà disciplinata da quest'ultima direttiva, in particolare dal suo articolo 15, paragrafo 1, letto alla luce degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta, oppure dal regolamento 2016/679, in particolare dall'articolo 23, paragrafo 1, di detto regolamento, letto alla luce delle medesime disposizioni della Carta.

203 Nel caso di specie, non si può escludere, come ha rilevato la Commissione europea nelle sue osservazioni scritte, che alcuni servizi ai quali si applica la normativa nazionale menzionata al punto 195 della presente sentenza costituiscano servizi di comunicazione elettronica ai sensi della direttiva 2002/58, circostanza che spetta al giudice del rinvio verificare.

204 A tal riguardo, occorre rilevare che nella direttiva 2002/58 rientrano i servizi di comunicazione elettronica che soddisfano le condizioni stabilite dall'articolo 2, lettera c), della direttiva 2002/21, al quale rinvia l'articolo 2 della direttiva 2002/58 e che definisce il servizio di comunicazione elettronica come «i servizi forniti di norma a pagamento consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva». Per quanto concerne i servizi della società dell'informazione, quali indicati ai punti 197 e 198 della presente sentenza e rientranti nella direttiva 2000/31, essi costituiscono servizi di comunicazione elettronica se consistono interamente o prevalentemente nella trasmissione di segnali su reti di comunicazione elettronica (v., in tal senso, sentenza del 5 giugno 2019, Skype Communications, C-142/18, EU:C:2019:460, punti 47 e 48).

205 Pertanto, i servizi di accesso a Internet, che sembrano rientrare nella normativa nazionale menzionata al punto 195 della presente sentenza, costituiscono, come conferma il considerando 10 della direttiva 2002/21, servizi di comunicazione elettronica ai sensi di detta direttiva (v., in tal senso, sentenza del 5 giugno 2019, Skype Communications, C-142/18, EU:C:2019:460, punto 37). Ciò vale anche per i servizi di posta elettronica su Internet, i quali, apparentemente, potrebbero del pari ricadere nell'ambito di applicazione della succitata normativa nazionale, dato che, sul piano tecnico, implicano interamente o prevalentemente la trasmissione di segnali su reti di comunicazione elettronica (v., in tal senso, sentenza del 13 giugno 2019, Google, C-193/18, EU:C:2019:498, punti 35 e 38).

206 Per quel che riguarda i requisiti risultanti 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, occorre rinviare all'insieme delle constatazioni e valutazioni operate nell'ambito della risposta fornita alle prime questioni nelle cause C-511/18 e C-512/18 nonché alle questioni prima e seconda nella causa C-520/18.

207 Quanto alle disposizioni derivanti dal regolamento 2016/679, occorre ricordare che quest'ultimo mira, in particolare, come emerge dal suo considerando 10, ad assicurare un livello elevato di protezione delle persone fisiche all'interno dell'Unione e, a tal fine, ad assicurare un'applicazione coerente e omogenea delle norme a protezione delle libertà e dei diritti fondamentali di tali persone con riguardo al trattamento dei dati personali in tutta l'Unione (v., in tal senso, sentenza del 16 luglio 2020, Facebook Ireland e Schrems, C-311/18, EU:C:2020:559, punto 101).

208 A tal fine, qualsiasi trattamento di dati personali deve rispettare, fatte salve le deroghe ex articolo 23 del regolamento 2016/679, i principi che disciplinano il trattamento dei dati personali nonché i diritti dell'interessato enunciati rispettivamente nei capi II e III di detto regolamento. In particolare, qualsiasi trattamento di dati personali deve essere conforme, da un lato, ai principi enunciati all'articolo 5 di tale regolamento e, dall'altro, soddisfare le condizioni di legittimazione elencate all'articolo 6 del medesimo regolamento (v., per analogia, relativamente alla direttiva 95/46, sentenza del 30 maggio 2013, Worten, C-342/12, EU:C:2013:355, punto 33 e giurisprudenza citata).

209 Per quanto riguarda, più in particolare, l'articolo 23, paragrafo 1, del regolamento 2016/679, occorre rilevare che esso, al pari di quanto stabilito dall'articolo 15, paragrafo 1, della direttiva 2002/58, consente agli Stati membri di limitare, alla luce delle finalità da esso contemplate e mediante misure legislative, la portata degli obblighi e dei diritti ivi previsti «qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare» la finalità perseguita. Qualsiasi misura legislativa adottata su questa base deve, in particolare, rispettare i requisiti specifici posti all'articolo 23, paragrafo 2, di detto regolamento.

210 Pertanto, l'articolo 23, paragrafi 1 e 2, del regolamento 2016/679 non può essere interpretato nel senso che può 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 (v., per analogia, relativamente alla direttiva 95/46, sentenza del 20 maggio 2003, Österreichischer Rundfunk e a., C-465/00, C-138/01 e C-139/01, EU:C:2003:294, punto 91). In particolare, analogamente a quanto vale per l'articolo 15, paragrafo 1, della direttiva 2002/58, il potere conferito agli Stati membri dall'articolo 23, paragrafo 1, del regolamento 2016/679 può essere esercitato soltanto nel rispetto del requisito di proporzionalità, secondo cui le deroghe e le restrizioni alla tutela dei dati personali devono operare entro i limiti dello stretto necessario (v., per analogia, relativamente alla direttiva 95/46, sentenza del 7 novembre 2013, IPI, C-473/12, EU:C:2013:715, punto 39 e giurisprudenza citata).

211 Ne consegue che le constatazioni e le valutazioni operate nell'ambito della risposta fornita alle prime questioni nelle cause C-511/18 e C-512/18 nonché alle questioni prima e seconda nella causa C-520/18 si applicano mutatis mutandis all'articolo 23 del regolamento 2016/679.

212 Alla luce delle considerazioni che precedono, occorre rispondere alla seconda questione nella causa C-512/18 dichiarando che la direttiva 2000/31 deve essere interpretata nel senso che essa non è applicabile in materia di tutela della riservatezza delle comunicazioni e delle persone fisiche con riguardo al trattamento dei dati personali nell'ambito dei servizi della società dell'informazione, essendo tale tutela disciplinata, a seconda dei casi, dalla direttiva 2002/58 o dal regolamento 2016/679. L'articolo 23, paragrafo 1, del regolamento 2016/679, letto alla luce degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta, deve essere interpretato nel senso che osta a 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.

Sulla terza questione nella causa C-520/18

213 Con la terza questione nella causa C-520/18, il giudice del rinvio chiede, in sostanza, se un giudice nazionale possa 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, nei confronti 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 relativi al traffico e dei dati relativi all'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.

214 Il principio del primato del diritto dell'Unione sancisce la preminenza del diritto dell'Unione sul diritto degli Stati membri. Tale principio impone pertanto a tutte le istituzioni degli Stati membri di dare pieno effetto alle varie norme dell'Unione, dato che il diritto degli Stati membri non può sminuire l'efficacia riconosciuta a tali differenti norme nel territorio dei suddetti Stati [sentenze del 15 luglio

1964, Costa, 6/64, EU:C:1964:66, pagg. 1143 e 1144, e del 19 novembre 2019, A.K. e a. (Indipendenza della Sezione disciplinare della Corte suprema), C-585/18, C-624/18 e C-625/18, EU:C:2019:982, punti 157 e 158 e giurisprudenza citata].

215 In base al principio del primato, ove non sia possibile procedere a un'interpretazione della normativa nazionale conforme alle prescrizioni del diritto dell'Unione, il giudice nazionale incaricato di applicare, nell'ambito della propria competenza, le disposizioni di diritto dell'Unione ha l'obbligo di garantire la piena efficacia delle medesime, disapplicando all'occorrenza, di propria iniziativa, qualsiasi disposizione contrastante della legislazione nazionale, anche posteriore, senza doverne chiedere o attendere la previa rimozione in via legislativa o mediante qualsiasi altro procedimento costituzionale [sentenze del 22 giugno 2010, Melki e Abdeli, C-188/10 e C-189/10, EU:C:2010:363, punto 43 e giurisprudenza citata; del 24 giugno 2019, Popławski, C-573/17, EU:C:2019:530, punto 58, e del 19 novembre 2019, A.K. e a. (Indipendenza della Sezione disciplinare della Corte suprema), C-585/18, C-624/18 e C-625/18, EU:C:2019:982, punto 160].

216 Solo la Corte può, eccezionalmente e per considerazioni imperative di certezza del diritto, concedere una sospensione provvisoria dell'effetto di disapplicazione esercitato da una norma di diritto dell'Unione rispetto a norme di diritto interno con essa in contrasto. Una siffatta limitazione nel tempo degli effetti dell'interpretazione data dalla Corte a tale diritto può essere concessa solo nella stessa sentenza che statuisce sull'interpretazione richiesta [v., in tal senso, sentenze del 23 ottobre 2012, Nelson e a., C-581/10 e C-629/10, EU:C:2012:657, punti 89 e 91; del 23 aprile 2020, Herst, C-401/18, EU:C:2020:295, punti 56 e 57, e del 25 giugno 2020, A e a. (Turbine eoliche di Aalter e Nevele), C-24/19, EU:C:2020:503, punto 84 e giurisprudenza citata].

217 Il primato e l'applicazione uniforme del diritto dell'Unione risulterebbero pregiudicati se i giudici nazionali avessero il potere di attribuire alle norme nazionali il primato, anche solo provvisoriamente, in caso di contrasto con il diritto dell'Unione (v., in tal senso, sentenza del 29 luglio 2019, Inter-Environnement Wallonie e Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, punto 177 e giurisprudenza citata).

218 Tuttavia, la Corte ha dichiarato, in una causa nella quale era in discussione la legittimità di misure adottate in violazione dell'obbligo sancito dal diritto dell'Unione di effettuare una valutazione preliminare delle incidenze di un progetto sull'ambiente e su un sito protetto, che un giudice nazionale può, se il diritto interno lo consente, eccezionalmente mantenere gli effetti di siffatte misure qualora tale mantenimento sia giustificato da considerazioni imperative connesse alla necessità di scongiurare una minaccia grave ed effettiva di interruzione dell'approvvigionamento di energia elettrica dello Stato membro interessato, cui non si potrebbe far fronte mediante altri mezzi e alternative, in particolare nell'ambito del mercato interno, e detto mantenimento può coprire soltanto il lasso di tempo strettamente necessario per porre rimedio a tale illegittimità (v., in tal senso, sentenza del 29 luglio 2019, Inter-Environnement Wallonie e Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, punti 175, 176, 179 e 181).

219 Orbene, a differenza dell'omissione di un obbligo procedurale quale la valutazione preliminare delle incidenze di un progetto nell'ambito specifico della tutela dell'ambiente, 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 può essere oggetto di regolarizzazione mediante una procedura analoga a quella menzionata al punto precedente. Infatti, il mantenimento degli effetti di una normativa nazionale, come quella di cui trattasi nei procedimenti principali, implicherebbe che detta normativa continui ad imporre ai fornitori di servizi di comunicazione elettronica obblighi che risultano contrari al diritto dell'Unione e comportano ingerenze gravi nei diritti fondamentali delle persone i cui dati sono stati conservati.

220 Pertanto, il giudice del rinvio non può 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, della legislazione nazionale di cui trattasi nei procedimenti principali.

221 Ciò premesso, nelle loro osservazioni presentate alla Corte, VZ, WY e XX sostengono che la terza questione solleva, implicitamente ma necessariamente, il problema se il diritto dell'Unione osti all'utilizzo, nell'ambito di un procedimento penale, di informazioni ed elementi di prova che sono stati ottenuti mediante una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione incompatibile con tale diritto.

222 A tal riguardo, e al fine di fornire una risposta utile al giudice del rinvio, occorre ricordare che, allo stato attuale del diritto dell'Unione, spetta, in linea di principio, esclusivamente al diritto nazionale determinare le norme relative all'ammissibilità e alla valutazione, nell'ambito di un procedimento penale avviato nei confronti di persone sospettate della commissione di reati gravi, di informazioni ed elementi di prova ottenuti mediante una siffatta conservazione di dati contraria al diritto dell'Unione.

223 Infatti, conformemente a una giurisprudenza costante, in assenza di una normativa dell'Unione in materia, spetta all'ordinamento giuridico interno di ciascuno Stato membro, ai sensi del principio dell'autonomia procedurale, 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) (v., in tal senso, sentenze del 6 ottobre 2015, Târşia, C-69/14, EU:C:2015:662, punti 26 e 27; del 24 ottobre 2018, XC e a., C-234/17, EU:C:2018:853, punti 21 e 22 e giurisprudenza citata, e del 19 dicembre 2019, Deutsche Umwelthilfe, C-752/18, EU:C:2019:1114, punto 33).

224 Per quanto concerne il principio di equivalenza, spetta al giudice nazionale investito di un procedimento penale fondato su informazioni o elementi di prova ottenuti in violazione dei requisiti risultanti dalla direttiva 2002/58 verificare se il diritto nazionale che disciplina tale procedimento preveda norme meno favorevoli riguardo all'ammissibilità e all'uso di tali informazioni ed elementi di prova rispetto a quelle che disciplinano le informazioni e gli elementi di prova ottenuti in violazione del diritto interno.

225 Quanto al principio di effettività, occorre rilevare che lo scopo delle norme nazionali relative all'ammissibilità e all'uso delle informazioni e degli elementi di prova consiste, in base alle scelte operate dal diritto nazionale, nell'evitare che informazioni ed elementi di prova ottenuti in modo illegittimo rechino indebitamente pregiudizio a una persona sospettata di avere commesso reati. Orbene, tale obiettivo può, secondo il diritto nazionale, essere raggiunto non solo con un divieto di utilizzare tali informazioni ed elementi di prova, ma altresì mediante norme e prassi nazionali che disciplinano la valutazione e la ponderazione delle informazioni e degli elementi di prova, o prendendo in considerazione il loro carattere illegittimo nell'ambito della determinazione della pena.

226 Ciò premesso, dalla giurisprudenza della Corte risulta che la necessità di escludere informazioni ed elementi di prova ottenuti in violazione delle prescrizioni del diritto dell'Unione deve essere valutata alla luce, in particolare, del rischio che l'ammissibilità di tali informazioni ed elementi di prova comporta per il rispetto del principio del contraddittorio e, pertanto, del diritto a un processo equo (v., in tal senso, sentenza del 10 aprile 2003, Steffensen, C-276/01, EU:C:2003:228, punti 76 e 77). Orbene, un giudice che ritenga che una parte non sia in grado di dedurre efficacemente in merito a un mezzo di prova che rientra in un settore che esula dalla competenza dei giudici e può influenzare in modo preponderante la valutazione dei fatti deve constatare una violazione del diritto a un processo equo ed escludere tale mezzo di prova al fine di evitare una violazione del genere (v., in tal senso, sentenza del 10 aprile 2003, Steffensen, C-276/01, EU:C:2003:228, punti 78 e 79).

227 Pertanto, il principio di effettività impone al giudice penale nazionale di non tenere conto degli elementi di prova ottenuti mediante una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'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 dette persone non siano in grado di prendere efficacemente posizione su tali informazioni ed elementi di prova, che provengono da un settore che esula dalla competenza dei giudici e possono influenzare in maniera preponderante la valutazione dei fatti.

228 Alla luce delle considerazioni che precedono, si deve rispondere alla terza questione nella causa C-520/18 dichiarando che un giudice nazionale non può applicare una disposizione del suo diritto nazionale che lo autorizzi a limitare nel tempo gli effetti di una dichiarazione di illegittimità ad esso incombente, in forza di tale diritto, nei confronti di una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica, a fini, in particolare, di salvaguardia della sicurezza nazionale e di lotta alla criminalità, una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione incompatibile 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. Detto articolo 15, paragrafo 1, interpretato alla luce del principio di effettività, impone al giudice penale nazionale di non tenere conto delle informazioni e degli elementi di prova ottenuti mediante una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione incompatibile con il diritto dell'Unione, nell'ambito di un procedimento penale avviato nei confronti di persone sospettate della commissione di reati, qualora dette persone non siano in grado di prendere efficacemente posizione su tali informazioni ed elementi di prova, che provengono da un settore che esula dalla competenza dei giudici e che possono influenzare in modo preponderante la valutazione dei fatti.

Sulle spese

229 Nei confronti delle parti nel procedimento principale la presente causa costituisce un incidente sollevato dinanzi al giudice del rinvio, cui spetta quindi statuire sulle spese. Le spese sostenute da altri soggetti per presentare osservazioni alla Corte non possono dar luogo a rifusione.

Per questi motivi, la Corte (Grande Sezione) dichiara:

1) **L'articolo 15, paragrafo 1, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa 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), come modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, letto alla luce degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, deve essere interpretato nel senso che osta a misure legislative che prevedono, ai fini di cui all'articolo 15, paragrafo 1, a titolo preventivo, una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione. Per contro, l'articolo 15, paragrafo 1, della direttiva 2002/58, come modificata dalla direttiva 2009/136, letto alla luce degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali, non osta a misure legislative**

   – **che consentano, a fini di salvaguardia della sicurezza nazionale, il 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, e 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;**

   – **che prevedano, a fini di salvaguardia della sicurezza nazionale, di lotta alle forme gravi di criminalità e di prevenzione delle minacce gravi alla sicurezza pubblica, una 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;**

   – **che prevedano, a fini di salvaguardia della sicurezza nazionale, di lotta alle forme gravi di criminalità e di prevenzione delle minacce gravi alla sicurezza pubblica, la conservazione generalizzata e indifferenziata degli indirizzi IP attribuiti all'origine di una connessione, per un periodo temporalmente limitato allo stretto necessario;**

   – **che prevedano, a fini di salvaguardia della sicurezza nazionale, di lotta alla criminalità e di salvaguardia della sicurezza pubblica, una conservazione generalizzata e indifferenziata dei dati relativi all'identità civile degli utenti di mezzi di comunicazione elettronica, e**

   – **che consentano, a fini di lotta alle forme gravi di criminalità e, a fortiori, di salvaguardia della sicurezza nazionale, il ricorso a un'ingiunzione che imponga ai fornitori di servizi di comunicazione elettronica, mediante un provvedimento dell'autorità competente soggetto 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 detti fornitori di servizi dispongono,**

   se tali misure garantiscono, 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.

2) **L'articolo 15, paragrafo 1, della direttiva 2002/58, come modificata dalla direttiva 2009/136, letto alla luce degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali, deve essere interpretato nel senso che non osta a una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica di ricorrere, da un lato, all'analisi automatizzata nonché alla raccolta in tempo reale, in particolare, dei dati relativi al traffico e dei dati relativi all'ubicazione e, dall'altro, alla raccolta in tempo reale dei dati tecnici relativi all'ubicazione delle apparecchiature terminali utilizzate, quando**

   – **il ricorso all'analisi automatizzata è limitato a situazioni nelle quali uno Stato membro si trova ad affrontare una minaccia grave per la sicurezza nazionale che si rivela reale e attuale o prevedibile e il ricorso a tale analisi può essere oggetto di un controllo effettivo, da parte di un giudice o di un organo amministrativo indipendente, la cui decisione è dotata di effetto vincolante, diretto a verificare l'esistenza di una situazione idonea a giustificare detta misura nonché il rispetto delle condizioni e delle garanzie che devono essere previste, e quando**

   – **il ricorso a una raccolta in tempo reale dei dati relativi al traffico e dei dati relativi all'ubicazione è limitato alle persone nei confronti delle quali esiste un valido motivo per sospettare che esse siano implicate, in un modo o nell'altro, in attività di terrorismo ed è soggetto a un controllo preventivo, effettuato da un giudice o da un organo amministrativo indipendente, la cui decisione ha effetto vincolante, al fine di accertarsi che tale raccolta in tempo reale sia autorizzata soltanto nei limiti di quanto strettamente necessario. In caso di emergenza debitamente giustificata, il controllo deve avvenire tempestivamente.**

3) **La 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 («Direttiva sul commercio elettronico»), deve essere interpretata nel senso che essa non è applicabile in materia di tutela della riservatezza delle comunicazioni e delle persone fisiche con riguardo al trattamento dei dati personali nell'ambito dei servizi della società dell'informazione, essendo tale tutela disciplinata, a seconda dei casi, dalla direttiva 2002/58, come modificata dalla direttiva 2009/136, o dal 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. L'articolo 23, paragrafo 1, del regolamento 2016/679, letto alla luce degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali, deve essere interpretato nel senso che osta a 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.**

4) **Un giudice nazionale non può applicare una disposizione del suo diritto nazionale che lo autorizzi a limitare nel tempo gli effetti di una dichiarazione di illegittimità ad esso incombente, in forza di tale diritto, nei confronti di una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica, a fini, in particolare, di salvaguardia della sicurezza nazionale e di lotta alla criminalità, una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione incompatibile con l'articolo 15, paragrafo 1, della direttiva 2002/58, come modificata dalla direttiva 2009/136, letto alla luce degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta. Detto articolo 15, paragrafo 1, interpretato alla luce del principio di effettività, impone al giudice penale nazionale di non tenere conto delle informazioni e degli elementi di prova ottenuti mediante una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione incompatibile con il diritto dell'Unione, nell'ambito di un procedimento penale avviato nei confronti di persone sospettate della commissione di reati,**

qualora dette persone non siano in grado di prendere efficacemente posizione su tali informazioni ed elementi di prova, che provengono da un settore che esula dalla competenza dei giudici e che possono influenzare in modo preponderante la valutazione dei fatti.

Firme