

- 2) L'articolo 15, paragrafo 1, della direttiva 2002/58, come modificata dalla direttiva 2009/136, letto alla luce dell'articolo 4, paragrafo 2, TUE nonché degli articoli 7, 8 e 11 e dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, dev'essere interpretato nel senso che osta a una normativa nazionale che consente a un'autorità statale di imporre, ai fini della salvaguardia della sicurezza nazionale, ai fornitori di servizi di comunicazione elettronica la trasmissione generalizzata e indifferenziata dei dati relativi al traffico e dei dati di ubicazione ai servizi di sicurezza e di intelligence.

(¹) GU C 22 del 22.1.2018.

Sentenza della Corte (Grande Sezione) del 6 ottobre 2020 (domande di pronuncia pregiudiziale del Conseil d'État e della Cour constitutionnelle — Belgio, Francia) — 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) / 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), Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX / Conseil des ministres

(Cause riunite C-511/18, C-512/18 e C-520/18) (¹)

(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 di 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, paragrafo 3, 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)

(2020/C 433/03)

Lingua processuale: il francese

Giudici del rinvio

Conseil d'État, Cour constitutionnelle

Parti

(Cause C-511/18 e C-512/18)

Ricorrenti: 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),

Convenuti: 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),

(Causa C-520/18)

Ricorrenti: Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX

Convenuto: Conseil des ministres

Con l'intervento di: Child Focus (C-520/18)

Dispositivo

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 di 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 di 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 di 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 di 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 di 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 di 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 di 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 di 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.

(¹) GU C 392 del 29.10.2018
GU C 408 del 12.11.2018