COMMISSIONE
EUROPEA

Bruxelles, 10.1.2017
COM(2017) 10 final

2017/0003 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche)

(Testo rilevante ai fini del SEE)

{SWD(2017) 3 final}
{SWD(2017) 4 final}
{SWD(2017) 5 final}
{SWD(2017) 6 final}

RELAZIONE

1. CONTESTO DELLA PROPOSTA

1.1. Motivi e obiettivi della proposta

La strategia per il mercato unico digitale[1] mira ad accrescere la fiducia nei servizi digitali nonché la sicurezza degli stessi. La riforma del quadro di riferimento per la tutela dei dati, in particolare l'adozione del regolamento (UE) 2016/679, il regolamento generale sulla protezione dei dati[2], costituiva un'azione fondamentale a tal fine. La strategia per il mercato unico digitale annunciava altresì il riesame della direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche[3], onde fornire un elevato livello di tutela della vita privata per gli utenti dei servizi di comunicazione elettronica e condizioni di parità per tutti gli operatori del mercato. La presente proposta riesamina la direttiva sulla vita privata elettronica, sulla scorta degli obiettivi fissati dalla strategia per il mercato unico digitale, onde garantire la coerenza con il regolamento generale sulla protezione dei dati.

La direttiva sulla vita privata elettronica garantisce la protezione dei diritti e delle libertà fondamentali, in particolare il rispetto della vita privata, la riservatezza delle comunicazioni e la tutela dei dati a carattere personale nel settore delle comunicazioni elettroniche. Essa garantisce altresì la libera circolazione dei dati, delle apparecchiature e dei servizi di comunicazione elettronica nell'Unione. Essa attua nel diritto derivato dell'Unione il diritto fondamentale al rispetto della vita privata relativamente alle comunicazioni, quale sancito all'articolo 7 della Carta dei diritti fondamentali dell'Unione europea ("**Carta**").

In linea con quanto disposto dalla comunicazione "Legiferare meglio", la Commissione ha eseguito *ex post* un programma di controllo dell'adeguatezza e dell'efficacia della regolamentazione ("**valutazione REFIT**") della direttiva sulla vita privata elettronica. Da tale valutazione emerge che gli obiettivi e i principi dell'attuale quadro di riferimento restano validi. Dall'ultima revisione della direttiva sulla vita privata elettronica nel 2009 sul mercato si sono tuttavia registrati importanti sviluppi tecnologici ed economici. I consumatori e le imprese si sono affidati sempre più ai nuovi servizi basati su internet intesi a consentire le comunicazioni interpersonali, quali il voice-over-IP, la messaggistica istantanea e i servizi di posta elettronica basati sulla rete anziché fruire dei servizi di comunicazione tradizionali. Questi servizi di comunicazione *over-the-top* ("**OTT**") non sono di norma soggetti all'attuale quadro di riferimento dell'Unione per le comunicazioni elettroniche, compresa la direttiva sulla vita privata elettronica. Ne consegue che la direttiva non è al passo con gli sviluppi tecnologici, il che si traduce in una lacuna nella tutela delle comunicazioni effettuate mediante i nuovi servizi.

---

1 Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni – Strategia per il mercato unico digitale in Europa, COM(2015) 192 final.

2 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

3 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 L 201 del 31.7.2002, pag. 37).

1.2. Coerenza con le disposizioni vigenti nel settore normativo interessato

La presente proposta, *lex specialis* nell'ambito del regolamento generale sulla protezione dei dati, disciplinerà e integrerà i dati afferenti alle comunicazioni elettroniche aventi carattere di dati personali. Tutte le questioni relative al trattamento dei dati personali non specificamente disciplinate dalla proposta lo sono dal suddetto regolamento. L'allineamento con il regolamento in questione ha comportato l'abrogazione di alcune disposizioni, quali gli obblighi di sicurezza di cui all'articolo 4 della direttiva.

1.3. Coerenza con le altre normative dell'Unione

La direttiva sulla vita privata elettronica costituisce parte del quadro regolamentare delle comunicazioni elettroniche. Nel 2016 la Commissione ha adottato la proposta di direttiva che istituisce il codice europeo delle comunicazioni elettroniche[4] che rivede tale quadro. Anche se la presente proposta non costituisce parte integrante del predetto codice, essa si fonda in parte sulle definizioni ivi contenute, inclusa quella di "servizi di comunicazione elettronica". Analogamente al codice europeo delle comunicazioni elettroniche, anche la presente proposta fa rientrare i fornitori di servizi OTT nel suo ambito d'applicazione al fine di rispecchiare la realtà del mercato. Il suddetto codice integra inoltre la presente proposta garantendo la sicurezza dei servizi di comunicazione elettronica.

La direttiva 2014/53/UE sulle apparecchiature radio[5] garantisce un mercato unico per tali apparecchiature. Essa dispone in particolare che, prima di essere immesse sul mercato, le apparecchiature radio contengano elementi di salvaguardia per garantire la tutela dei dati personali e della vita privata dell'utente. Nell'ambito della direttiva sulle apparecchiature radio e del regolamento (UE) n. 1025/2012 sulla normazione europea[6] la Commissione dispone del potere di adottare misure. La presente proposta non incide sulla direttiva sulle apparecchiature radio.

La proposta non contiene disposizioni specifiche in materia di conservazione dei dati. Essa mantiene l'essenza dell'articolo 15 della direttiva sulla vita privata elettronica, allineandosi con il testo specifico dell'articolo 23 del regolamento generale sulla protezione dei dati, che disciplina i motivi per i quali gli Stati membri possono restringere l'ambito di applicazione dei diritti e degli obblighi in articoli specifici della direttiva sulla vita privata elettronica. Gli Stati membri sono pertanto liberi di mantenere o creare quadri di riferimento nazionali in materia di conservazione dei dati che prevedano fra l'altro misure di conservazione mirate, purché essi siano conformi al diritto dell'Unione e tengano conto della giurisprudenza della Corte di giustizia sull'interpretazione della direttiva sulla vita privata elettronica e della carta dei diritti fondamentali[7].

---

4 Proposta di direttiva del Parlamento europeo e del Consiglio che istituisce il codice europeo delle comunicazioni elettroniche (rifusione) (COM/2016/0590 final - 2016/0288 (COD)).

5 Direttiva 2014/53/UE del Parlamento europeo e del Consiglio, del 16 aprile 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio e che abroga la direttiva 1999/5/CE (GU L 153 del 22.5.2014, pag. 62).

6 Regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio (GU L 316 del 14.11.2012, pag. 12).

7 Cfr. cause riunite C-293/12 e C-594/12 *Digital Rights Ireland e Seitlinger et al.*, ECLI:EU:C:2014:238; cause riunite C-203/15 e C-698/15 *Tele2 Sverige AB e Secretary of State for the Home Department*, ECLI:EU:C:2016:970.

La proposta infine non si applica alle attività delle istituzioni, degli organi e delle agenzie dell'Unione. I suoi principi e i relativi obblighi, per quanto attiene al diritto al rispetto della vita privata e alle comunicazioni in relazione al trattamento dei dati delle comunicazioni elettroniche, sono stati tuttavia inclusi nella proposta di regolamento che abroga il regolamento (CE) n. 45/2001[8].

2. BASE GIURIDICA, SUSSIDIARIETÀ E PROPORZIONALITÀ

2.1. Base giuridica

La presente proposta si basa sugli articoli 16 e 114 del trattato sul funzionamento dell'Unione europea ("**TFUE**").

L'articolo 16 del TFUE introduce una base giuridica specifica per stabilire le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni e degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Poiché una comunicazione elettronica che interessa una persona fisica è di norma considerata un dato personale, la tutela di tali persone fisiche con riguardo alla riservatezza delle comunicazioni e al trattamento di tali dati dovrebbe essere basata sull'articolo 16.

La proposta mira inoltre a tutelare le comunicazioni e i relativi interessi legittimi delle persone giuridiche. Il senso e la portata dei diritti di cui all'articolo 7 della Carta sono, conformemente all'articolo 52, paragrafo 3, della stessa, uguali a quelli sanciti all'articolo 8, paragrafo 1, della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali ("**CEDU**"). Per quanto concerne l'ambito di applicazione dell'articolo 7 della Carta, la giurisprudenza della Corte di giustizia dell'Unione europea[9] ("**CGUE**") e della Corte europea dei diritti dell'uomo[10] conferma che le attività professionali delle persone giuridiche non possono essere escluse dalla tutela dei diritti garantita dall'articolo 7 della Carta e dell'articolo 8 della CEDU.

Poiché l'iniziativa ha doppia finalità e la componente relativa alla tutela delle comunicazioni delle persone giuridiche nonché l'obiettivo di realizzare il mercato interno per tali comunicazioni elettroniche per garantirne il funzionamento a tale proposito non può essere considerata puramente accessoria, l'iniziativa dovrebbe di conseguenza essere basata anche sull'articolo 114 del TFUE.

2.2. Sussidiarietà

Il rispetto delle comunicazioni è un diritto fondamentale sancito dalla Carta. Il contenuto delle comunicazioni elettroniche può rivelare informazioni altamente sensibili relative agli utenti finali coinvolti nella comunicazione. Analogamente, i metadati derivati dalle comunicazioni elettroniche possono anch'essi rivelare informazioni estremamente sensibili e personali, come espressamente riconosciuto dalla CGUE[11]. La maggioranza degli Stati membri riconosce

---

8 Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati (GU L 8 del 12.1.2001, pag. 1).

9 Cfr. C-450/06 *Varec SA*, ECLI:EU:C:2008:91, punto 48.

10 Cfr. fra l'altro, ECHR, sentenze *Niemietz contro Germania*, sentenza del 16 dicembre 1992, serie A n° 251-B, punto 29; *Société Colas Est et al. contro Francia*, n. 37971/97, punto 41; ECHR 2002-III; *Peck contro Regno Unito*, n. 44647/98, punto 57, ECHR 2003-I; nonché *Vinci Construction e GTM Génie Civil et Services contro Francia*, nn. 63629/10 e 60567/10, punto 63, 2 aprile 2015.

11 Cfr. nota a piè di pagina 7.

inoltre l'esigenza di tutelare le comunicazioni come diritto costituzionale distinto. Anche se è possibile che gli Stati membri adottino politiche volte a garantire che tale diritto non sia violato, questo risultato non sarebbe uniforme in assenza di norme dell'Unione e si creerebbero restrizioni ai flussi transfrontalieri di dati personali e non personali connessi all'uso di servizi di comunicazione elettronica. Infine, per mantenere la coerenza con il regolamento generale sulla protezione dei dati, è necessario riesaminare la direttiva sulla vita privata elettronica e adottare misure atte ad allineare i due strumenti.

Gli sviluppi tecnologici e gli obiettivi della strategia per il mercato unico digitale hanno rafforzato la necessità di agire a livello dell'Unione. Il successo del mercato unico digitale nell'UE dipende dall'efficacia dell'UE nell'abbattere ostacoli e barriere nazionali, per sfruttare i vantaggi e le economie di tale mercato europeo. Inoltre, poiché le tecnologie internet e digitali non conoscono frontiere, la dimensione della problematica va oltre il territorio di un unico Stato membro. Considerata la situazione attuale gli Stati membri non possono risolvere efficacemente i problemi. Requisiti per un corretto funzionamento del mercato unico digitale sono eque condizioni per gli operatori di mercato che forniscono servizi sostituibili e un'identica tutela degli utenti finali a livello dell'Unione.

2.3. Proporzionalità

Onde garantire un'efficace tutela giuridica del rispetto della vita privata e delle comunicazioni, è necessario ampliare l'ambito di applicazione dei fornitori di servizi OTT. Anche se diversi dei principali fornitori OTT rispettano già in toto o in parte il principio di riservatezza delle comunicazioni, la tutela dei diritti fondamentali non può essere lasciata all'autoregolamentazione del settore. Riveste inoltre crescente importanza la tutela efficace della vita privata in relazione alle apparecchiature terminali, divenute indispensabili nella vita personale e professionale per lo stoccaggio di informazioni sensibili. L'attuazione della direttiva sulla vita privata elettronica non è stata efficace nei confronti degli utenti finali. Pertanto l'attuazione del principio del consenso centralizzato nei programmi e il relativo invito rivolto all'utente a impostare le informazioni relative alla vita privata sono necessari per realizzare l'obiettivo. L'applicazione del presente regolamento è affidata alle autorità di controllo e al meccanismo di coerenza del regolamento generale sulla protezione dei dati. La proposta consente inoltre agli Stati membri di adottare misure nazionali in deroga per specifici fini legittimi. La proposta pertanto non va oltre quanto necessario per conseguire l'obiettivo in ottemperanza al principio di proporzionalità enunciato all'articolo 5 del trattato sull'Unione europea. Gli obblighi imposti ai servizi interessati sono mantenuti al livello più basso possibile, senza ledere i diritti fondamentali in questione.

2.4. Scelta dell'atto giuridico

La Commissione presenta una proposta di regolamento al fine di garantire la coerenza con il regolamento generale sulla protezione dei dati e la certezza del diritto nei confronti degli utenti e delle imprese evitando un'interpretazione divergente fra Stati membri. Un regolamento è in grado di garantire un pari livello di tutela degli utenti in tutta l'Unione e costi di conformità inferiori per le imprese con attività transfrontaliere.

3. RISULTATI DELLE VALUTAZIONI EX POST, DELLE CONSULTAZIONI DEI PORTATORI DI INTERESSI E DELLE VALUTAZIONI D'IMPATTO

3.1. Valutazioni *ex post* / Vaglio di adeguatezza della legislazione vigente

La valutazione REFIT ha esaminato l'efficienza della direttiva sulla vita privata elettronica nel contribuire a un'adeguata tutela del rispetto della vita privata e della riservatezza delle comunicazioni nell'UE, cercando inoltre di identificare eventuali ridondanze.

La valutazione REFIT ha concluso che gli obiettivi della direttiva illustrati sopra restano **pertinenti**. Mentre il regolamento generale sulla protezione dei dati personali garantisce la tutela di tali dati, la direttiva sulla vita privata elettronica garantisce la riservatezza delle comunicazioni, che possono anche contenere dati non personali e dati connessi a una persona giuridica. Uno strumento distinto dovrebbe quindi garantire una tutela efficace dell'articolo 7 della Carta. Altre disposizioni, quali le norme sull'invio di comunicazioni commerciali indesiderate, si sono dimostrate ancora pertinenti.

In termini di **efficacia ed efficienza** dalla valutazione REFIT è emerso che la direttiva non ha pienamente realizzato gli obiettivi prefissati. La stesura poco chiara di alcune disposizioni e l'ambiguità dei concetti giuridici hanno compromesso l'armonizzazione, creando così problemi alle imprese che svolgono attività frontaliere. La valutazione ha inoltre dimostrato che alcune disposizioni hanno creato oneri inutili per le imprese e i consumatori. A titolo di esempio, la norma sul consenso intesa a tutelare la riservatezza delle apparecchiature terminali non è riuscita a realizzare gli obiettivi, in quanto gli utenti finali si trovano di fronte a richieste di accettare i marcatori ("cookie di tracciatura") senza capirne il senso e, talvolta, sono addirittura esposti ai cookie senza dare il loro consenso. La norma sul consenso è sovrabbondante, poiché riguarda anche le pratiche non lesive della vita privata, ma è nel contempo sottodimensionata in quanto chiaramente non disciplina alcune tecniche di tracciamento (per es. le impronte digitali per accedere al dispositivo) che possono non contemplare l'accesso al dispositivo e/o lo stoccaggio nello stesso. L'attuazione può infine risultare gravosa per le imprese.

La valutazione ha concluso che le norme sulla vita privata elettronica posseggono ancora un **valore aggiunto per l'UE** per realizzare meglio l'obiettivo di garantire la vita privata in linea alla luce di un mercato delle comunicazioni elettroniche sempre più transnazionale. Essa ha anche dimostrato che nel complesso tali norme sono coerenti con altra legislazione pertinente, anche se sono state identificate alcune ridondanze rispetto al nuovo regolamento generale sulla protezione dei dati (cfr. sezione 1.2).

3.2. Consultazioni delle parti interessate

La Commissione ha organizzato una consultazione pubblica che si è svolta fra il 12 aprile e il 5 luglio 2016, in occasione della quale sono pervenuti 421 contributi[12]. Di seguito se ne enumerano le risultanze principali[13].

– **Esigenza di norme speciali per il settore delle comunicazioni elettroniche per quanto riguarda la riservatezza delle stesse:** l'83,4% dei cittadini, delle organizzazioni dei consumatori e della società civile e l'88,9% delle autorità pubbliche che hanno risposto si dichiarano d'accordo, mentre il 63,4% del settore si dichiara non d'accordo.

– **Ampliamento dell'ambito di applicazione ai nuovi servizi di comunicazione (OTT):** il 76% dei cittadini e della società civile e il 93,1% delle autorità pubbliche si dichiarano d'accordo, mentre solo il 36,2% dei rispondenti del settore è favorevole a questo ampliamento.

[12] 162 contributi provenienti da cittadini, 33 dalla società civile e dalle organizzazioni dei consumatori, 186 dal settore e 40 dalle autorità pubbliche, comprese le competenti autorità responsabili dell'applicazione della direttiva sulla vita privata elettronica.

[13] La relazione completa è disponibile al seguente indirizzo: https://ec.europa.eu/digital-single-market/news-redirect/37204.

– **Modifica delle esenzioni per consentire il trattamento dei dati relativi al traffico e alla localizzazione:** il 49,1% dei cittadini e delle organizzazioni dei consumatori e della società civile nonché il 36% delle autorità pubbliche preferiscono non ampliare le esenzioni, mentre il 36% del settore si dichiara a favore di tale ampliamento; 2/3 del settore auspicano l'abrogazione pura e semplice delle disposizioni.

– **Sostegno alle soluzioni proposte relativamente alla questione del consenso ai marcatori:** l'81,2% dei cittadini e il 63% delle autorità pubbliche sostengono l'imposizione di obblighi ai fabbricanti di apparecchiature terminali affinché commercializzino prodotti con impostazioni di vita privata attive preimpostate, mentre il 58,3% del settore appoggia l'opzione di autoregolamentazione e/o coregolamentazione.

Nell'aprile 2016 la Commissione europea ha inoltre organizzato due seminari, uno aperto a tutte le parti interessate e uno riservato alle autorità nazionali competenti, durante i quali sono state trattate le questioni oggetto della consultazione pubblica. I pareri espressi in queste occasioni rispecchiavano l'esito della consultazione pubblica.

Per ottenere le opinioni dei cittadini è stata effettuata in tutta l'UE un'indagine Eurobarometro sulla vita privata elettronica[14]. Di seguito se ne enumerano le risultanze principali[15].

– Per il 78% è molto importante che l'accesso alle informazioni personali contenute nel computer, nel cellulare o nel tablet sia subordinato al consenso.

– Il 72% ritiene molto importante che sia garantita la riservatezza della posta elettronica e della messaggistica istantanea in linea.

– L'89% concorda con l'opzione suggerita, ossia che le impostazioni predefinite del loro navigatore prevedano il rifiuto della condivisione delle informazioni.

3.3. Raccolta e uso di perizie

La Commissione si è basata sulle seguenti consulenze.

– Consultazioni mirate di gruppi di esperti dell'UE: parere del gruppo di lavoro "Articolo 29"; parere del GEPD; parere della piattaforma REFIT; opinioni del BEREC; opinioni dell'ENISA e di membri della rete di cooperazione per la tutela dei consumatori.

– Consulenza esterna, in particolare i due studi in appresso:

  – studio "ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation" (SMART 2013/007116);

  – studio "Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector" (SMART 2016/0080).

3.4. Valutazione d'impatto

Per questa proposta è stata effettuata una valutazione d'impatto in merito alla quale il 28 settembre 2016 il comitato per il controllo normativo ha emesso un parere favorevole[16]. Al

[14] Indagine Eurobarometro 2016 (EB 443) sulla vita privata elettronica (SMART 2016/079).

[15] La relazione completa è disponibile al seguente indirizzo: https://ec.europa.eu/digital-single-market/news-redirect/37205.

[16] http://ec.europa.eu/transparency/regdoc/?fuseaction=ia.

fine di dar seguito alle raccomandazioni del comitato, la valutazione d'impatto spiega meglio l'ambito di applicazione dell'iniziativa, la sua coerenza con altri strumenti giuridici (regolamento generale sulla protezione dei dati, codice europeo delle comunicazioni elettroniche, direttiva sulle apparecchiature radio) e la necessità di uno strumento distinto. Lo scenario di riferimento è ulteriormente elaborato e chiarito. L'analisi degli impatti è irrobustita e riequilibrata, chiarendo e rafforzando la descrizione dei costi e dei benefici previsti.

Sono state esaminate le seguenti opzioni strategiche secondo i criteri di efficacia, efficienza e coerenza.

– **Opzione 1:** misure non legislative (non vincolanti);

– **Opzione 2:** rafforzamento limitato della vita privata/riservatezza e semplificazione;

– **Opzione 3:** rafforzamento moderato della vita privata/riservatezza e semplificazione;

– **Opzione 4:** rafforzamento significativo della vita privata/riservatezza e semplificazione;

– **Opzione 5:** abrogazione della direttiva sulla vita privata elettronica.

Per molti aspetti l'**opzione 3** è stata scelta come **opzione privilegiata** per raggiungere gli obiettivi tenendone in considerazione l'efficienza e la coerenza. In appresso i principali vantaggi.

– Rafforzamento della tutela della riservatezza delle comunicazioni elettroniche grazie a un ampliamento dell'ambito di applicazione dello strumento giuridico per includere nuovi servizi di comunicazione elettronica equivalenti sotto il profilo funzionale. Il regolamento aumenta inoltre il controllo da parte dell'utente finale, chiarendo che il consenso può essere espresso attraverso opportune impostazioni tecniche.

– Rafforzamento della tutela dalle comunicazioni indesiderate, grazie all'introduzione di un obbligo di pubblicizzazione dell'identificativo del chiamante o un prefisso obbligatorio per le chiamate di natura commerciale nonché maggiori possibilità di bloccare le chiamate provenienti da numeri indesiderati.

– Semplificazione e chiarimento dell'ambiente regolamentare restringendo il margine di manovra lasciato agli Stati membri, abrogando le disposizioni obsolete e ampliando le eccezioni alle norme sul consenso.

L'impatto economico dell'opzione 3 dovrebbe essere nel complesso proporzionato agli obiettivi della proposta. Le opportunità commerciali connesse al trattamento dei dati delle comunicazioni sono aperte ai servizi di comunicazione elettronica tradizionale mentre i fornitori di servizi OTT si trovano soggetti alla medesima regolamentazione. Ne consegue che questi operatori dovranno affrontare alcuni costi di conformità supplementari. Tale cambiamento non inciderà tuttavia in modo sostanziale sugli operatori OTT che già operano sulla base del consenso. Infine, l'impatto dell'opzione non sarebbe percepito negli Stati membri che hanno già esteso queste norme ai servizi OTT.

Grazie alla centralizzazione del consenso nei programmi di navigazione internet, alla richiesta agli utenti di scegliere le proprie impostazioni di vita privata e all'estensione delle eccezioni alla norma del consenso ai marcatori, una proporzione significativa di imprese potrebbe eliminare gli avvisi e le strisce sui marcatori, ottenendo così, in potenza, un risparmio in termini di costi e una semplificazione di rilievo. Può tuttavia diventare più difficile per la pubblicità mirata in linea ottenere il consenso se un'ingente proporzione di utenti sceglie l'impostazione di rifiutare i marcatori di terzi. Nel contempo la centralizzazione del consenso

non impedisce agli operatori del sito web di ottenere il consenso per mezzo di richieste individuali agli utenti, mantenendo così l'attuale modello commerciale. Per alcuni fornitori di navigatori o programmi analoghi ne deriverebbero costi supplementari in quanto dovrebbero garantire impostazioni orientate al rispetto della vita privata.

Lo studio esterno ha identificato tre diversi scenari di attuazione dell'opzione 3, subordinatamente all'entità responsabile della finestra di dialogo fra l'utente che ha scelto di rifiutare i marcatori di terzi o di adottare le impostazioni di non tracciamento e i siti web visitati che invitano l'utente a riconsiderare la propria scelta. I soggetti cui potrebbe essere eventualmente affidato questo compito tecnico sono: 1) i programmi come i navigatori internet; 2) i tracciatori di terzi; 3) i singoli siti web (per es. il servizio di società dell'informazione richiesto dall'utente). L'opzione 3 comporterebbe un risparmio complessivo, in termini di conformità rispetto all'ipotesi di riferimento, pari al 70% (948,8 milioni di euro di risparmio) del primo scenario (navigatore), attuata nella presente proposta. I risparmi in termini di costi sarebbero inferiori negli altri scenari. Poiché tali risparmi complessivi derivano da un decremento molto significativo del numero di imprese interessate, l'importo individuale dei costi di conformità per ciascuna impresa sarebbe mediamente più elevato di oggi.

3.5. Efficienza normativa e semplificazione

Le misure strategiche proposte nell'opzione preferita affrontano l'obiettivo della semplificazione e della riduzione degli oneri amministrativi, in linea con i risultati della valutazione REFIT e con il parere della piattaforma REFIT[17].

La piattaforma REFIT ha emesso tre insiemi di raccomandazioni alla Commissione:

– la tutela della vita privata del cittadino dovrebbe essere rafforzata allineando la direttiva sulla vita privata elettronica al regolamento generale sulla protezione dei dati;

– l'efficacia della tutela dei cittadini contro la commercializzazione indesiderata dovrebbe essere rafforzata attraverso l'aggiunta di eccezioni alla norma sul consenso per i marcatori;

– la Commissione affronta i problemi connessi all'attuazione nazionale e agevola lo scambio delle migliori pratiche fra gli Stati membri.

La proposta include nella fattispecie:

– l'uso di definizioni neutre sul piano tecnologico per ricomprendere tecnologie e servizi nuovi al fine di garantire che il regolamento sia adeguato alle esigenze future;

– l'abrogazione delle norme di sicurezza per eliminare la duplicazione regolamentare;

– il chiarimento dell'ambito di applicazione per aiutare a eliminare/ridurre il rischio di interpretazione divergente da parte degli Stati membri (punto 3 del parere);

– il chiarimento e la semplificazione della norma sul consenso per l'uso dei marcatori e altri identificativi, come illustrato nelle sezioni 3.1 e 3.4 (punto 2 del parere);

– l'allineamento delle autorità di controllo alle autorità competenti per l'applicazione del regolamento generale sulla protezione dei dati e il meccanismo di coerenza dello stesso regolamento.

[17] http://ec.europa.eu/smart-regulation/refit/refit-platform/docs/recommendations/opinion_comm_net.pdf.

3.6. Impatto sui diritti fondamentali

La proposta mira a rendere più efficace e ad aumentare il livello di tutela della vita privata e dei dati personali trattati in relazione alle comunicazioni elettroniche ai sensi degli articoli 7 e 8 della Carta e a garantire una maggiore certezza del diritto. La proposta integra e disciplina il regolamento generale sulla protezione dei dati. Una tutela efficace della riservatezza delle comunicazioni è fondamentale per esercitare la libertà di espressione e di informazione nonché altri diritti connessi, quali il diritto alla tutela dei dati personali o alla libertà di pensiero, coscienza e religione.

4. INCIDENZA SUL BILANCIO

Nessuna.

5. ALTRI ELEMENTI

5.1. Piani attuativi e modalità di monitoraggio, valutazione e informazione

La Commissione monitorerà l'applicazione del regolamento e ogni tre anni presenterà una relazione di valutazione al Parlamento europeo, al Consiglio e al Comitato economico e sociale. Queste relazioni saranno rese pubbliche e illustreranno in dettaglio l'effettiva applicazione del regolamento.

5.2. Illustrazione dettagliata delle disposizioni specifiche della proposta

Il capo I reca le disposizioni generali: l'oggetto (articolo 1), l'ambito di applicazione (articoli 2 e 3) e le relative definizioni, compresi i riferimenti alle pertinenti definizioni provenienti da altri strumenti dell'UE, come il regolamento generale sulla protezione dei dati.

Il capo II contiene le disposizioni principali volte a garantire la riservatezza delle comunicazioni elettroniche (articolo 5) e i fini limitati consentiti e le condizioni di trattamento dei dati di tali comunicazioni (articoli 6 e 7). Esso disciplina altresì la protezione delle apparecchiature terminali, i) garantendo l'integrità delle informazioni ivi conservate e ii) proteggendo le informazioni provenienti dall'attrezzatura terminale, in quanto possono consentire l'identificazione dell'utente finale (articolo 8). Infine l'articolo 9 disciplina in modo particolareggiato il consenso degli utenti finali, un elemento lecito del presente regolamento, facente riferimento esplicito alla sua definizione e alle condizioni derivate dal regolamento generale sulla protezione dei dati, mentre l'articolo 10 impone un obbligo ai fornitori di programmi di comunicazione elettronica di aiutare gli utenti finali a definire in modo efficace le impostazioni relative alla vita privata. L'articolo 11 disciplina in modo particolareggiato le finalità e le condizioni in cui gli Stati membri possono restringere le predette disposizioni.

Il capo III disciplina i diritti degli utenti finali a controllare l'invio e la ricezione di comunicazioni elettroniche per tutelare la propria vita privata: i) il diritto degli utenti finali di impedire la presentazione dell'identificazione della linea chiamante per garantire l'anonimato (articolo 12) e le relative limitazioni (articolo 13); e ii) l'obbligo imposto ai fornitori di comunicazione interpersonale basate sul numero pubblicamente disponibile di prevedere la possibilità di limitare il ricevimento di chiamate indesiderate (articolo 14). Questo capo disciplina altresì la condizioni alle quali gli utenti finali possono essere inclusi negli elenchi pubblici (articolo 15) e le condizioni alle quali si possono effettuare comunicazioni indesiderate a fini di commercializzazione diretta (articolo 17). Esso è altresì connesso ai rischi per la sicurezza e contempla un obbligo per i fornitori di servizi di comunicazione elettronica di avvertire gli utenti finali in caso di rischio particolare suscettibile di

compromettere la sicurezza della rete e dei servizi. Gli obblighi di sicurezza contenuti nel regolamento generale sulla protezione dei dati e nel codice europeo delle comunicazioni elettroniche saranno applicabili ai fornitori di servizi di comunicazione elettronica.

Il capo IV disciplina il controllo e l'applicazione di questo regolamento, affidandoli alle autorità di controllo responsabili del regolamento generale sulla protezione dei dati, considerate le forti sinergie esistenti fra le questioni connesse alla tutela dei dati in generale e quelle connesse alla riservatezza delle comunicazioni (articolo 18). I poteri del Comitato europeo per la protezione dei dati sono ampliati (articolo 19) e la cooperazione e il meccanismo di coerenza previsti nel regolamento generale sulla protezione dei dati saranno applicabili in caso di questioni transfrontaliere connesse a questo regolamento (articolo 20).

Il capo V disciplina in modo particolareggiato i diversi rimedi a disposizione degli utenti finali (articoli 21 e 22) nonché le sanzioni che possono essere imposte (articolo 24), comprese le condizioni generali per imporre sanzioni amministrative pecuniarie (articolo 23).

Il capo VI disciplina l'adozione degli atti delegati e di esecuzione, ai sensi degli articoli 290 e 291 del trattato.

Infine, il capo VII contiene le disposizioni finali del regolamento: l'abrogazione della direttiva sulla vita privata elettronica, il monitoraggio e il riesame, l'entrata in vigore e l'applicazione. Per quanto concerne il riesame, la Commissione intende valutare fra l'altro se sia ancora necessario un atto giuridico distinto, alla luce degli sviluppi giuridici, tecnici o economici e tenuto conto della prima valutazione del regolamento (UE) 2016/679, prevista entro il 25 maggio 2020.

2017/0003 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche)

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare gli articoli 16 e 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo[1],

visto il parere del Comitato delle regioni[2],

visto il parere del Garante europeo della protezione dei dati[3],

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

1) L'articolo 7 della Carta dei diritti fondamentali dell'Unione europea ("Carta") tutela il diritto fondamentale di ogni persona al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni. Il rispetto della riservatezza delle comunicazioni rappresenta una dimensione essenziale di tale diritto. La riservatezza delle comunicazioni elettroniche garantisce che le informazioni scambiate fra le parti e gli elementi esterni di tale comunicazione, compresi il momento, l'origine dell'invio e il destinatario, non siano rivelate a nessun'altra parte che non sia coinvolta nella comunicazione. Il principio di riservatezza dovrebbe applicarsi agli attuali e ai futuri mezzi di comunicazione, ivi compresi le chiamate, l'accesso a internet, le applicazioni di messaggistica istantanea, la posta elettronica, le chiamate telefoniche via internet e la messaggistica personale attraverso le piattaforme sociali.

2) Il contenuto delle comunicazioni elettroniche può rivelare informazioni altamente sensibili in merito alle persone fisiche coinvolte nella comunicazione, dalle esperienze personali e le emozioni alle condizioni mediche, le preferenze sessuali e le opinioni politiche, la divulgazione delle quali potrebbe tradursi in un danno personale e sociale, in una perdita economica o nell'imbarazzo. Analogamente, i metadati derivati dalle comunicazioni elettroniche possono anch'essi rivelare informazioni estremamente sensibili e personali. Tali metadati includono i numeri chiamati, i siti web visitati, la

[1] GU C del , pag. .
[2] GU C del , pag. .
[3] GU C del , pag. .

geolocalizzazione, l'ora, la data e la durata di una chiamata effettuata, ecc., consentendo di trarre conclusioni precise relativamente alla vita privata delle persone coinvolte nella comunicazione elettronica, come le loro relazioni sociali, le loro abitudini e attività quotidiane, i loro interessi, gusti, ecc.

3) I dati delle comunicazioni elettroniche possono altresì rivelare informazioni relative a entità giuridiche, come secreti aziendali o altre informazioni sensibili aventi valore economico. Pertanto le disposizioni del presente regolamento dovrebbero applicarsi sia alle persone fisiche, sia alle persone giuridiche. Il presente regolamento dovrebbe inoltre garantire che le disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio[4] si applichino anche agli utenti finali aventi natura di persone giuridiche. Questo include la definizione di consenso contenuta nel regolamento (UE) 2016/679. Qualora si faccia riferimento al consenso di un utente finale, comprese le persone giuridiche, si dovrebbe applicare tale definizione. Le persone giuridiche dovrebbero inoltre godere degli stessi diritti degli utenti finali aventi natura di persone fisiche per quanto attiene alle autorità di controllo; inoltre, le autorità di controllo ai sensi del presente regolamento dovrebbero essere responsabili anche del monitoraggio dell'applicazione del presente regolamento nei confronti delle persone giuridiche.

4) Ai sensi dell'articolo 8, paragrafo 1, della Carta e dell'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea, ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. Il regolamento (UE) 2016/679 stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché norme relative alla libera circolazione di tali dati. I dati delle comunicazioni elettroniche possono includere i dati personali ai sensi del regolamento (UE) 2016/679.

5) Le disposizioni del presente regolamento precisano e integrano le norme generali sulla protezione dei dai personali stabilite dal regolamento (UE) 2016/679 per quanto riguarda i dati afferenti alle comunicazioni elettroniche aventi carattere di dati personali. Il presente regolamento non abbassa pertanto il livello di tutela delle persone fisiche previsto dal regolamento (UE) 2016/679. Il trattamento dei dati delle comunicazioni elettroniche da parte dei fornitori di servizi di comunicazioni elettroniche dovrebbe essere consentito solo in conformità al presente regolamento.

6) Se da un lato i principi e le disposizioni principali della direttiva 2002/58/CE del Parlamento europeo e del Consiglio[5] restano generalmente validi, dall'altro tuttavia la direttiva non è stata interamente al passo con l'evoluzione della realtà tecnologica e di mercato, il che si è tradotto in una tutela incoerente o non abbastanza efficace della vita privata e della riservatezza delle comunicazioni elettroniche. Tali sviluppi comprendono l'entrata sul mercato dei servizi di comunicazione elettronica che dal punto di vista del consumatore sono in grado di sostituire i servizi tradizionali ma che non sono soggetti al medesimo insieme di norme. Un ulteriore sviluppo riguarda le nuove tecniche che consentono di tracciare il comportamento in linea degli utenti

[4] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

[5] 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 L 201 del 31.7.2002, pag. 37).

finali, questione non disciplinata dalla direttiva 2002/58/CE. La direttiva 2002/58/CEE dovrebbe pertanto essere abrogata e sostituita dal presente regolamento.

7) Entro i limiti consentiti dal presente regolamento, agli Stati membri dovrebbe essere consentito mantenere o introdurre disposizioni nazionali per precisare ulteriormente e chiarire l'applicazione delle norme del presente regolamento al fine di garantire un'applicazione effettiva nonché l'interpretazione di tali norme. Pertanto il margine di discrezionalità degli Stati membri dovrebbe mantenere un equilibrio fra la tutela della vita privata e dei dati personali e la libera circolazione dei dati delle comunicazioni elettroniche.

8) Il presente regolamento dovrebbe applicarsi ai fornitori di servizi di comunicazioni elettroniche, ai fornitori di elenchi pubblici e ai fornitori di programmi che consentono le comunicazioni elettroniche, compresi il recupero e la presentazione delle informazioni in rete. Il presente regolamento dovrebbe inoltre applicarsi alle persone fisiche e giuridiche che fruiscono di servizi di comunicazioni elettroniche per inviare comunicazioni commerciali a fini di commercializzazione diretta o per raccogliere informazioni connesse alle apparecchiature terminali degli utenti finali o conservate nelle stesse.

9) Il presente regolamento dovrebbe applicarsi anche ai dati delle comunicazioni elettroniche elaborati in relazione alla fornitura e alla fruizione dei servizi di comunicazione elettronica nell'Unione, indipendentemente dal fatto che il trattamento avvenga nell'Unione o no. Inoltre, al fine di non privare gli utenti finali di una tutela efficace, il presente regolamento dovrebbe applicarsi anche ai dati delle comunicazioni elettroniche elaborati in relazione alla fornitura di servizi di comunicazione elettronica erogati al di fuori dell'Unione a utenti finali ubicati nell'Unione.

10) Le apparecchiature radio e il relativo software commercializzati nel mercato interno dell'Unione devono essere conformi alla direttiva 2014/53/UE del Parlamento europeo e del Consiglio[6]. Il presente regolamento non dovrebbe incidere sull'applicabilità dei requisiti della direttiva 2014/53/UE né sui poteri della Commissione di adottare atti delegati a norma della medesima direttiva, imponendo che categorie specifiche o classi di apparecchiature radio siano munite di salvaguardie volte a garantire la tutela dei dati personali e la vita privata degli utenti finali.

11) I servizi fruiti a fini di comunicazione e i pertinenti mezzi tecnici di erogazione hanno avuto un'importante evoluzione. Gli utenti finali sostituiscono sempre più la telefonia tradizionale, i messaggi di testo (SMS) e i servizi di trasmissione di posta elettronica con servizi in linea equivalenti, quali il *voice-over-IP*, i servizi di messaggistica e i servizi di posta elettronica basati sul web. Al fine di garantire una protezione efficace ed equa degli utenti finali quando fruiscono di servizi equivalenti sotto il profilo funzionale, il presente regolamento si avvale della definizione di servizi di comunicazione elettronica stabilita nella [direttiva del Parlamento europeo e del Consiglio che istituisce il codice europeo delle comunicazioni elettroniche[7]]. Tale definizione comprende non solo i servizi di accesso a internet e i servizi che consistono interamente o parzialmente nella trasmissione di segnali ma anche i servizi

---

6 Direttiva 2014/53/UE del Parlamento europeo e del Consiglio, del 16 aprile 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio e che abroga la direttiva 1999/5/CE (GU L 153 del 22.5.2014, pag. 62).

7 Proposta di direttiva del Parlamento europeo e del Consiglio che istituisce il codice europeo delle comunicazioni elettroniche (rifusione) (COM/2016/0590 final – 2016/0288 (COD)).

di comunicazione interpersonale che possono anche essere basati sul numero, quali per es. il *voice-over-IP*, i servizi di messaggistica e i servizi di posta elettronica basati sul web. La tutela della riservatezza delle comunicazioni è fondamentale anche per quanto riguarda i servizi di comunicazione interpersonale accessori di altri servizi; pertanto dovrebbero essere disciplinati dal presente regolamento tali tipi di servizi aventi anche una funzionalità di comunicazione.

12) I dispositivi e le macchine connessi comunicano sempre più fra loro per mezzo di reti di comunicazione elettroniche (internet delle cose). La trasmissione di comunicazioni da macchina a macchina prevede la trasmissione di segnali attraverso una rete e quindi costituisce un servizio di comunicazione elettronica. Al fine di garantire la piena tutela della vita privata e della riservatezza delle comunicazioni, nonché promuovere un internet delle cose affidabile e sicuro nel mercato unico digitale, è necessario chiarire che il presente regolamento dovrebbe applicarsi alla trasmissione di comunicazioni da macchina a macchina. Pertanto il principio di riservatezza sancito dal presente regolamento dovrebbe applicarsi anche alla trasmissione di comunicazioni da macchina a macchina. Si potrebbero altresì adottare salvaguardie specifiche nell'ambito della legislazione settoriale, quale per esempio la direttiva 2014/53/UE.

13) Lo sviluppo di tecnologie senza filo veloci ed efficienti ha promosso una maggior disponibilità di accessi pubblici alla rete grazie alle reti senza fili accessibili in spazi pubblici e semi-privati, come gli "hotspot" ubicati in diversi luoghi nelle città, nei grandi magazzini, nei centri commerciali e negli ospedali. Nella misura in cui tali reti di comunicazione sono accessibili a un gruppo indefinito di utenti finali,, dovrebbe essere tutelata la riservatezza delle comunicazioni trasmesse attraverso tali reti. Il fatto che i servizi di comunicazione elettronica senza fili possano essere accessori di altri servizi non dovrebbe ostacolare la garanzia della tutela della riservatezza dei dati delle comunicazioni e dell'applicazione del presente regolamento. Il presente regolamento dovrebbe pertanto applicarsi ai dati delle comunicazioni elettroniche che si avvalgono dei servizi di comunicazione elettronica e delle reti di comunicazione pubbliche. Il presente regolamento non dovrebbe tuttavia applicarsi a gruppi chiusi di utenti finali, quali le reti aziendali, il cui accesso è limitato ai membri dell'impresa.

14) I dati delle comunicazioni elettroniche dovrebbero essere definiti in modo sufficientemente ampio e tecnologicamente neutro da ricomprendere tutte le informazioni relative al contenuto trasmesso o scambiato (contenuto delle comunicazioni elettroniche) nonché le informazioni relative a un utente finale di servizi di comunicazione elettronica trattati al fine di trasmettere, distribuire o consentire lo scambio di contenuto delle comunicazioni elettroniche, compresi i dati atti a tracciare e identificare la fonte e la destinazione di una comunicazione, l'ubicazione geografica nonché la data, l'ora, la durata e il tipo di comunicazione. Che i segnali siano trasmessi via filo, onde radio, mezzi ottici o elettromagnetici, comprese le reti satellitari, le reti cablate, le reti terrestri fisse (a commutazione di circuito e a commutazione di pacchetto, compreso internet) e mobili, i sistemi di cavi elettrici, i dati relativi a tali segnali dovrebbero essere considerati metadati di comunicazioni elettroniche e quindi soggetti alle disposizioni del presente regolamento. I metadati delle comunicazioni elettroniche possono includere informazioni che costituiscono parte dell'abbonamento al servizio nel momento in cui tali informazioni sono elaborate ai fini di trasmissione, distribuzione o scambio di contenuto di comunicazioni elettroniche.

15) I dati delle comunicazioni elettroniche dovrebbero essere trattati in modo riservato. Questo significa che, senza il consenso di tutte le parti coinvolte, dovrebbe essere

proibita qualsiasi interferenza con la trasmissione dei dati delle comunicazioni elettroniche, sia direttamente con intervento umano o attraverso l'elaborazione automatizzata con macchine. Il divieto di intercettazione dei dati delle comunicazioni dovrebbe applicarsi durante la loro trasmissione, ossia fino alla ricezione del contenuto della comunicazione elettronica da parte del destinatario previsto. L'intercettazione dei dati delle comunicazioni elettroniche potrebbe avvenire, per esempio, quando una parte diversa dalle parti coinvolte nella comunicazione ascolta le chiamate, effettua la scansione o conserva il contenuto delle comunicazioni elettroniche o i metadati associati a fini diversi dallo scambio di comunicazioni. L'intercettazione avviene altresì quando terzi monitorano i siti web visitati, la tempistica delle visite, l'interazione con altri, ecc. senza il consenso dell'utente finale interessato. Mano a mano che la tecnologia evolve, aumentano anche le modalità tecniche di effettuare l'intercettazione. Queste modalità spaziano dall'installazione di attrezzature che raccolgono i dati da un'apparecchiatura terminale in zone mirate, quali i cosiddetti numeri IMSI (International Mobile Subscriber Identity) a programmi e tecniche che, per esempio, monitorano surrettiziamente le abitudini di navigazione al fine di creare profili di utenti finali. Fra gli altri esempi di intercettazione si annoverano la cattura dei dati del carico o i dati del contenuto da reti senza filo non cifrate, comprese le abitudini di navigazione, senza il consenso degli utenti finali.

16) Il divieto di memorizzare comunicazioni 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. Non dovrebbe proibire neppure il trattamento dei dati delle comunicazioni elettroniche atto a garantire la sicurezza e la continuità dei servizi di comunicazione elettronica, fra cui il controllo delle minacce alla sicurezza come la presenza di software maligni o il trattamento dei metadati per garantire i requisiti necessari di qualità del servizio, quali la latenza, il jitter, ecc.

17) Il trattamento dei dati delle comunicazioni elettroniche può essere utile per le imprese, i consumatori e la società nel suo complesso. Rispetto alla direttiva 2002/58/CE il presente regolamento amplia le possibilità per i fornitori di servizi di comunicazione elettronica di trattare i metadati delle comunicazioni elettroniche, previo consenso degli utenti finali. Gli utenti finali attribuiscono tuttavia grande importanza alla riservatezza delle loro comunicazioni, comprese le loro attività in linea e al fatto di voler controllare l'uso dei dati afferenti alle comunicazioni elettroniche a fini diversi dalla trasmissione della comunicazione. Il presente regolamento dovrebbe quindi imporre ai fornitori di servizi di comunicazione elettronica di ottenere il consenso degli utenti finali al trattamento dei metadati delle comunicazioni elettroniche, che dovrebbe includere i dati sull'ubicazione del dispositivo generati al fine di ottenere e mantenere l'accesso e la connessione al servizio. I dati relativi alla localizzazione generati diversi da quelli connessi all'ambito della fornitura di servizi di comunicazione elettronica non dovrebbero essere considerati metadati. Fra gli esempi di usi commerciali dei metadati delle comunicazioni elettroniche da parte dei fornitori di servizi di comunicazione elettronica si può annoverare la fornitura di mappe di calore, ossia una rappresentazione grafica dei dati per mezzo di colori che indicano la presenza di persone. Per mostrare i movimenti del traffico in alcune direzioni durante un determinato intervallo, è necessario un identificativo per collegare la posizione delle persone nei diversi intervalli. Tale identificativo mancherebbe se si usassero dati anonimi e il movimento non potrebbe essere visualizzato. Un siffatto uso dei metadati delle comunicazioni elettroniche potrebbe per esempio avvantaggiare le autorità pubbliche e gli operatori dei trasporti pubblici per definire gli sviluppi delle nuove

infrastrutture in base all'uso e alla pressione sulle strutture esistenti. Laddove un tipo di trattamento dei metadati delle comunicazioni elettroniche, in particolare se ciò avviene per mezzo delle nuove tecnologie e tenuto contro della natura, dell'ambito di applicazione, del contesto e dei fini del trattamento, è suscettibile di comportare un elevato rischio per i diritti e le libertà delle persone fisiche, si dovrebbe effettuare una valutazione d'impatto sulla protezione dei dati ed eventualmente consultare l'autorità di controllo, prima del trattamento, a norma degli articoli 35 e 36 del regolamento (UE) 2016/679.

18) Gli utenti finali possono acconsentire al trattamento dei loro metadati per ricevere servizi specifici quali i servizi di protezione da attività fraudolente (mediante analisi dei dati di utilizzo, della localizzazione e del conto cliente in tempo reale). Nell'economia digitale i servizi sono spesso erogati dietro corrispettivo non monetario, per esempio esponendo gli utenti finali a messaggi pubblicitari. Ai fini del presente regolamento il consenso dell'utente o dell'abbonato, senza considerare se quest'ultimo sia una persona fisica o giuridica, dovrebbe avere lo stesso significato del consenso della persona interessata a norma del regolamento 2016/679. I servizi di accesso a internet a banda larga e di comunicazione vocale vanno considerati servizi essenziali per le persone affinché possano comunicare e partecipare ai vantaggi dell'economia digitale. Il consenso al trattamento dei dati provenienti dall'utilizzo di internet o delle comunicazioni vocali non sarà valido se il titolare dei dati non dispone di una vera scelta libera o se non può rifiutare o revocare il consenso senza conseguenze negative.

19) Il contenuto delle comunicazioni elettroniche afferisce all'essenza del diritto fondamentale al rispetto della vita privata e familiare, del domicilio e delle comunicazioni tutelato dall'articolo 7 della Carta. Eventuali interferenze con il contenuto delle comunicazioni elettroniche dovrebbero essere ammesse solo in condizioni definite molto chiaramente, per fini specifici e subordinatamente ad adeguate salvaguardie contro gli abusi. Il presente regolamento stabilisce la possibilità che i fornitori di servizi di comunicazione elettronica trattino i dati delle comunicazioni elettroniche in transito con il consenso informato di tutti gli utenti finali interessati. A titolo di esempio, i fornitori possono offrire servizi che comportano la scansione dei messaggi di posta elettronica per rimuovere un dato materiale predeterminato. Considerata la sensibilità del contenuto delle comunicazioni, il presente regolamento parte dal presupposto che il trattamento di tali dati relativi al contenuto comporti rischi elevati per i diritti e le libertà delle persone fisiche. Quando effettua il trattamento di tali tipi di dati, il fornitore del servizio di comunicazione elettronica dovrebbe sempre consultare l'autorità di controllo prima del trattamento. Tale consultazione dovrebbe avvenire a norma dell'articolo 36, paragrafi 2 e 3, del regolamento (UE) 2016/679. Tale presunzione non dovrebbe comprendere il trattamento dei dati relativi al contenuto utili all'erogazione di un servizio richiesto dall'utente finale se questi ha acconsentito a detto trattamento ed esso è effettuato ai fini e per la durata strettamente necessari e proporzionati per il servizio in questione. Dopo la trasmissione del contenuto delle comunicazioni elettroniche da parte dell'utente finale e il ricevimento da parte del o degli utenti finali previsti, tale contenuto può essere registrato o conservato dal o dagli utenti finali oppure da terzi, abilitati a registrare o conservare tali dati. Il trattamento di tali dati deve essere conforme al regolamento (UE) 2016/679.

20) Le apparecchiature terminali degli utenti finali delle reti di comunicazione elettronica e qualsiasi informazione connessa all'uso di tali apparecchiature, in particolare

conservata in tali apparecchiature o da esse emessa o richiesta o trattata per consentire il collegamento a un'altra apparecchiatura e/o ad apparecchiature di rete, rientrano nella sfera privata degli utenti finali per i quali si richiede la tutela ai sensi della Carta dei diritti fondamentali dell'Unione europea e della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Considerato che tali apparecchiature contengono o trattano informazioni suscettibili di rivelare dettagli relativi alle complessità emotive, politiche, sociali di una persona, compreso il contenuto delle comunicazioni, immagini, l'ubicazione delle persone mediante l'accesso alle capacità GPS del dispositivo, gli elenchi di contatti e altre informazioni in esso già conservate, le informazioni connesse a tale apparecchiatura necessitano di una tutela rafforzata della vita privata. Inoltre, i cosiddetti programmi spia, i bachi invisibili ("web bugs"), gli identificatori occulti e altri dispositivi analoghi possono introdursi nell'apparecchiatura terminale dell'utente finale a sua insaputa al fine di avere accesso ad informazioni, archiviare informazioni occulte o seguire le attività dell'utente. Le informazioni relative al dispositivo dell'utente finale possono anche essere raccolte in remoto a fini di identificazione e tracciabilità, mediante il ricorso a tecniche quali le impronte digitali per accedere al dispositivo, spesso senza la consapevolezza dell'utente finale e possono seriamente compromettere la vita privata di tali utenti finali. Le tecniche che monitorano surrettiziamente le azioni degli utenti finali, per esempio tracciandone le attività in linea o l'ubicazione della loro apparecchiatura terminale o che compromettono il funzionamento di tale apparecchiatura costituiscono una grave minaccia per la vita privata degli utenti finali. Pertanto qualsiasi interferenza con l'apparecchiatura terminale dell'utente finale dovrebbe essere consentita solo con il consenso dell'utente finale e a fini specifici e trasparenti.

21) Le eccezioni all'obbligo di ottenere il consenso per avvalersi delle capacità di trattamento e conservazione dell'apparecchiatura terminale o per accedere alle informazioni in essa conservate dovrebbero essere limitate alle situazioni che comportano un'intrusione nella vita privata scarsa o nulla. Nella fattispecie, il consenso non dovrebbe essere richiesto per autorizzare la conservazione tecnica o l'accesso strettamente necessario e proporzionato per l'uso legittimo di consentire l'uso di un servizio specifico espressamente richiesto dall'utente finale. Vi si può includere la conservazione dei marcatori per la durata di un'unica sessione stabilita su un sito web per tenere traccia di quanto inserito dall'utente finale in moduli in linea su diverse pagine. I marcatori possono anche costituire uno strumento legittimo e utile, per esempio per misurare il traffico in un sito. L'attività di controllo di configurazione da parte dei fornitori di servizi della società dell'informazione per erogare il servizio conformemente alle impostazioni dell'utente finale e la semplice registrazione del fatto che il dispositivo dell'utente finale non sia abilitato a ricevere il contenuto richiesto dall'utente finale non dovrebbero configurare un accesso a detto dispositivo o un uso delle capacità di elaborazione del dispositivo.

22) I metodi usati per fornire le informazioni e ottenere il consenso dell'utente finale dovrebbero essere il più possibile intuitivi. Considerata la diffusione dei marcatori e di altre tecniche di tracciatura, gli utenti finali ricevono sempre più richieste di consenso per conservare tali marcatori di tracciatura nelle apparecchiature terminali. Di conseguenza gli utenti finali sono subissati di richieste di consenso. L'uso di mezzi tecnici per dare il consenso, per esempio mediante impostazioni trasparenti e intuitive, può contribuire a risolvere il problema. Il presente regolamento dovrebbe pertanto contemplare la possibilità di esprimere il consenso mediante le apposite impostazioni di un navigatore o di un'altra applicazione. Le scelte degli utenti finali nelle

impostazioni relative alla vita privata di un navigatore o di un'altra applicazione dovrebbero essere vincolanti e applicabili nei confronti di terzi. I navigatori di rete sono un tipo di programma applicativo che consente di recuperare e presentare informazioni presenti sulla rete. Altri tipi di applicazioni, quali quelle che consentono di chiamare e scambiare messaggi o fornire indicazioni stradali, dispongono delle stesse capacità. I navigatori fungono da intermediario fra quanto avviene presso l'utente finale e il sito web. Da questa prospettiva si trovano in una posizione privilegiata per ricoprire un ruolo attivo nell'aiutare l'utente finale a controllare il flusso di informazioni da e verso l'apparecchiatura terminale. Più particolarmente, i navigatori web possono essere usati come controlli all'accesso, aiutando così gli utenti finali ad evitare che le informazioni relative alla loro apparecchiatura terminale (per es. cellulare, tablet o computer) siano consultate o conservate.

23) I principi della protezione dei dati fin dalla progettazione e protezione per impostazione predefinita sono disciplinati all'articolo 25 del regolamento (UE) 2016/679. Attualmente le impostazioni predefinite per i marcatori nella maggior parte dei navigatori sono del tipo "accetta tutti i marcatori". I fornitori di programmi che consentono il recupero e la presentazione di informazioni presenti in rete dovrebbero quindi essere obbligati a configurare il programma affinché esso preveda l'opzione volta a impedire che terzi conservino informazioni sull'apparecchiatura terminale, spesso presentata come "rifiuta tutti i marcatori di terzi". Gli utenti finali dovrebbero avere a disposizione un insieme di opzioni di impostazione della vita privata comprese fra la più restrittiva (per es. "non accettare mai marcatori") e la meno restrittiva (per es. "accetta sempre i marcatori") e una posizione intermedia (per es. "rifiuta i marcatori di terzi" o "accetta solo i marcatori di prima parte"). Tali impostazioni della vita privata dovrebbero essere presentate in modo facilmente visibile e intelligibile.

24) Affinché i navigatori possano ottenere il consenso degli utenti finali ai sensi del regolamento (UE) 2016/679, per esempio, per conservare i marcatori di terzi, essi dovrebbero fra l'altro, richiedere un'azione chiara e affermativa da parte dell'utente finale dell'apparecchiatura terminale a significare il libero accordo, specificamente informato e univoco, alla conservazione e all'accesso di tali marcatori da e verso l'apparecchiatura terminale. Tale azione può essere considerata affermativa per esempio se gli utenti finali sono tenuti a selezionare attivamente l'opzione "accetta marcatori di terzi" per confermare il loro accordo, ricevendo informazioni sufficienti per effettuare la scelta. A tal fine è necessario che i fornitori di programmi che consentono l'accesso a internet, al momento dell'installazione informino gli utenti finali della possibilità di scegliere le impostazioni relative alla vita privata fra le diverse opzioni, chiedendo loro di effettuare una selezione. Le informazioni comunicate non dovrebbero dissuadere gli utenti finali dal selezionare le impostazioni di vita privata più restrittive e dovrebbero includere informazioni pertinenti in merito ai rischi associati al consenso a conservare i marcatori di terzi nel computer, compresa la compilazione di registri di lungo periodo contenenti la cronologia di navigazione sul lungo periodo degli utenti e l'uso di tali dati per presentare pubblicità mirata. I navigatori sono invitati a dotarsi di modi semplici per modificare le impostazioni di vita privata in qualsiasi momento durante l'uso e consentire all'utente di consentire eccezioni (elenco positivo) per taluni siti web o specificare quali marcatori di siti web (terzi) si accettano o si rifiutano.

25) L'accesso alle reti di comunicazione elettronica esige l'emissione regolare di alcuni pacchetti di dati al fine di aprire o mantenere una connessione con la rete o con altri dispositivi della rete. I dispositivi devono inoltre disporre di un indirizzo unico

assegnato onde essere identificabili su tale rete. Gli standard senza filo e cellulari contemplano analoghe emissioni di segnali attivi contenenti identificativi unici, quali un indirizzo MAC, i codici IMEI (International Mobile Station Equipment Identity), IMSI, ecc. Un'unica stazione di base senza filo (ossia un'emittente e una ricevente), come un punto d'accesso senza filo, ha un intervallo specifico entro il quale tali informazioni possono essere catturate. Esistono fornitori di servizi che offrono servizi di tracciamento sulla base della scansione delle informazioni connesse all'apparecchiatura con diverse funzionalità, compreso il conteggio delle persone, la comunicazione di dati relativi al numero di persone in attesa??, la determinazione del numero di persone presenti in una data zona, ecc. Tali informazioni possono essere usate a fini più intrusivi, come l'invio di messaggi commerciali agli utenti finali, per esempio al momento in cui entrano nei negozi, con offerte personalizzate. Anche se alcune di queste funzionalità non comportano rischi elevati per la vita privata, altre possono essere lesive, come per esempio quelle che tracciano le persone nel tempo, anche in merito a visite ripetute di luoghi specifici. I fornitori che seguono queste pratiche dovrebbero affiggere avvisi ben visibili al limitare della zona coperta con i quali si informano gli utenti finali che entrano nella zona delimitata che la tecnologia è operativa entro un dato perimetro, la finalità del tracciamento, il nominativo del responsabile e l'esistenza di eventuali misure a disposizione dell'utente finale per minimizzare o bloccare la raccolta. Qualora siano raccolti dati personali a norma dell'articolo 13 del regolamento (UE) 2016/679 si dovrebbero comunicare informazioni supplementari.

26) Laddove il trattamento dei dati delle comunicazioni elettroniche da parte dei fornitori di servizi di comunicazione elettronica rientra nell'ambito di applicazione del presente regolamento, questo dovrebbe prevedere la possibilità che l'Unione o gli Stati membri, a determinate condizioni, possano limitare i diritti e gli obblighi, qualora tale restrizione costituisca una misura necessaria e proporzionata all'interno di una società democratica per la salvaguardia di specifici interessi pubblici, compresa la sicurezza nazionale, la difesa, la sicurezza pubblica nonché la prevenzione, la ricerca, l'accertamento o il perseguimento dei reati o l'esecuzione di sanzioni penali, compresa la salvaguardia e la prevenzione delle minacce alla sicurezza pubblica e ad altri obiettivi di rilievo di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un interesse economico o finanziario importante dell'Unione o di uno Stato membro, o un monitoraggio, un'ispezione o una funzione regolatrice connessa all'esercizio dell'autorità ufficiale competente per tali interessi. Il presente regolamento non pregiudica quindi la facoltà degli Stati membri di effettuare intercettazioni legali di comunicazioni elettroniche o di adottare altre misure, se necessario e proporzionato, a salvaguardia degli interessi pubblici suddetti, conformemente alla Carta dei diritti fondamentali dell'Unione europea e alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, nell'interpretazione della Corte di giustizia dell'Unione europea e della Corte europea dei diritti dell'uomo. I fornitori di servizi di comunicazione elettronica dovrebbero prevedere procedure apposite per agevolare le richieste legittime delle autorità competenti, se pertinente, anche tenendo conto del ruolo del rappresentante designato a norma dell'articolo 3, paragrafo 3.

27) Con riguardo all'identificazione della linea chiamante è necessario tutelare il diritto dell'autore della chiamata di impedire che sia indicata la linea dalla quale si effettua la chiamata, nonché il diritto del chiamato di respingere chiamate da linee non identificate. Alcuni utenti finali, in particolare le linee di assistenza e servizi analoghi, hanno interesse a garantire l'anonimato dei loro chiamanti. Con riferimento

all'identificazione della linea collegata, è necessario tutelare il diritto e il legittimo interesse del chiamato a sopprimere la presentazione della linea alla quale il chiamante è realmente collegato.

28) In casi specifici esistono giustificati motivi per disattivare la soppressione della presentazione della linea chiamante. Il diritto alla vita privata degli utenti finali riguardo all'identificazione della linea chiamante dovrebbe essere limitato allorché ciò sia necessario per identificare le chiamate importune e, riguardo all'identificazione della linea chiamante e ai dati relativi all'ubicazione, se necessario per consentire ai servizi di emergenza (come eCall) di svolgere il loro compito nel modo più efficace possibile.

29) Esiste una tecnologia che consente ai fornitori di servizi di comunicazione elettronica di limitare in diversi modi il ricevimento di chiamate indesiderate da parte degli utenti finali, bloccando le chiamate silenziose e altre chiamate fraudolente e importune. I fornitori di servizi di comunicazione interpersonale basata sul numero accessibili al pubblico dovrebbero dotarsi di tale tecnologia e tutelare a titolo gratuito gli utenti finali dalle chiamate importune. I fornitori dovrebbero garantire che gli utenti finali siano consapevoli dell'esistenza di tali funzionalità, per esempio pubblicizzandole sul loro sito web.

30) Gli elenchi pubblici di utenti finali di servizi di comunicazione elettronica sono ampiamente disponibili. Per elenco pubblico si intende qualsiasi elenco o servizio che contiene informazioni relative agli utenti finali, quali il numero di telefono (anche cellulare), i recapiti di posta elettronica e i servizi di consultazione elenchi. Il diritto alla vita privata e alla tutela dei dati personali di una persona fisica prevede di richiedere il consenso agli utenti finali aventi natura di persone fisiche prima di inserire tali dati in un elenco. Il legittimo interesse delle persone giuridiche prevede che gli utenti finali aventi natura di persone giuridiche abbiano il diritto di contestare che i dati a esse relativi siano inseriti in un elenco.

31) Se gli utenti finali aventi natura di persone fisiche acconsentono all'inserimento dei loro dati in tali elenchi, essi dovrebbero poter determinare su base consensuale quali categorie di dati personali siano incluse nell'elenco (per es. nome, indirizzo di posta elettronica, nome utente, numero di telefono). I fornitori di elenchi pubblici dovrebbero inoltre informare gli utenti finali delle finalità di tale elenco e delle funzioni di ricerca prima di inserirli in detto elenco. Gli utenti finali dovrebbero poter determinare mediante consenso sulla base di quali categorie di dati personali è possibile effettuare una ricerca nei recapiti. Le categorie di dati personali inseriti nell'elenco e le categorie di dati personali in base alle quali possono essere ricercati i recapiti dell'utente finale non devono essere necessariamente le stesse.

32) Nel presente regolamento per commercializzazione diretta si intende qualsiasi forma di pubblicità mediante la quale una persona fisica o giuridica invia comunicazioni di commercializzazione diretta direttamente a uno o più utenti finali identificati o identificabili, per mezzo di servizi di comunicazione elettronica. Oltre all'offerta di prodotti e servizi a fini commerciali, si dovrebbero altresì includere i messaggi inviati da partiti politici che contattano le persone fisiche attraverso servizi di comunicazione elettronica al fine di promuovere il loro partito. Analogamente, dovrebbe essere così per i messaggi inviati da organizzazioni senza fini di lucro a sostegno delle finalità dell'organizzazione.

33) Si dovrebbero prevedere salvaguardie a tutela degli utenti finali contro le comunicazioni indesiderate a fini di commercializzazione diretta che costituiscono

un'intrusione nella vita privata degli utenti finali. Il grado di intrusione nella vita privata e di disturbo è considerato abbastanza simile indipendentemente dall'ampia gamma di tecnologie e canali usati per trasmettere tali comunicazioni elettroniche, siano essi sistemi automatici di chiamata e comunicazione, applicazioni di messaggistica istantanea, posta elettronica, SMS, MMS, Bluetooth, ecc. Si giustifica pertanto la richiesta di consenso all'utente finale prima di inviare comunicazioni elettroniche commerciali a fini di commercializzazione diretta al fine di tutelare le persone dall'intrusione nella loro vita privata nonché il loro interesse legittimo. La certezza del diritto e la necessità di garantire che le norme che tutelano dalle comunicazioni elettroniche indesiderate siano "a prova di futuro" giustificano l'esigenza di definire un unico insieme di norme che non varino a seconda della tecnologia usata per trasmettere tali comunicazioni non richieste, garantendo nel contempo un livello di tutela equivalente per tutti i cittadini in tutta l'Unione. È tuttavia ragionevole consentire l'uso dei recapiti di posta elettronica nell'ambito di una relazione commerciale esistente finalizzato alla proposta di prodotti o servizi analoghi. Tale possibilità dovrebbe applicarsi alla stessa impresa che ha ottenuto i recapiti elettronici a norma del regolamento (UE) 2016/679.

34) Se gli utenti finali hanno espresso il loro consenso a ricevere comunicazioni indesiderate a fini di commercializzazione diretta, essi dovrebbero poter avere ancora la facoltà di revocare agevolmente tale consenso in qualsiasi momento. Al fine di facilitare l'attuazione efficace delle norme dell'Unione in materia di messaggi indesiderati a scopi di commercializzazione diretta, è necessario proibire l'occultamento dell'identità, gli indirizzi o i numeri di risposta falsi allorché sono inviati messaggi commerciali indesiderati a scopi di commercializzazione diretta. Le comunicazioni di commercializzazione diretta indesiderate dovrebbero pertanto essere chiaramente riconoscibili come tali e dovrebbero indicare l'identità della persona fisica o giuridica che trasmette la comunicazione o per conto della quale tale comunicazione è trasmessa, nonché fornire informazioni ai destinatari affinché possano esercitare il loro diritto di opporsi a ricevere ulteriori messaggi commerciali scritti e/o orali.

35) Onde consentire di revocare agevolmente il consenso, le persone fisiche o giuridiche che inviano comunicazioni di commercializzazione diretta dovrebbero visualizzare un collegamento o un indirizzo di posta elettronica valido di facile fruizione affinché gli utenti finali possano revocare il loro consenso. Le persone fisiche o giuridiche che inviano comunicazioni di commercializzazione diretta mediante chiamate vocali e chiamate effettuate da sistemi automatici di chiamata e comunicazione dovrebbero visualizzare il loro identificativo di linea al quale l'impresa può essere contattata o presentare un codice specifico che identifichi il fatto che la chiamata ha carattere commerciale.

36) Le chiamate vocali di commercializzazione diretta che non comportano l'uso di sistemi automatici di chiamata e comunicazione hanno un costo maggiore per l'emittente senza imporre oneri finanziari agli utenti finali. Gli Stati membri dovrebbero quindi essere in grado di istituire o mantenere sistemi nazionali che autorizzano tali chiamate unicamente destinate agli utenti che non hanno obiettato.

37) I fornitori di servizi che offrono servizi di comunicazione elettronica dovrebbero informare gli utenti finali delle misure a loro disposizione per proteggere la sicurezza delle loro comunicazioni, ad esempio attraverso l'uso di particolari tipi di programmi o tecniche di cifratura. L'obbligo di informare gli utenti finali su particolari rischi relativi alla sicurezza non esonera il fornitore di servizi dall'obbligo di prendere, a sue

proprie spese, provvedimenti adeguati ed immediati per rimediare a tutti i nuovi rischi imprevisti relativi alla sicurezza e ristabilire il normale livello di sicurezza del servizio. La fornitura all'abbonato di informazioni sui rischi relativi alla sicurezza dovrebbe essere gratuita. La sicurezza è valutata alla luce dell'articolo 32 del regolamento (UE) 2016/679.

38) Onde garantire la piena coerenza con il regolamento (UE) 2016/679 l'applicazione delle disposizioni del presente regolamento dovrebbe essere affidata alle stesse autorità responsabili dell'applicazione delle disposizioni di detto regolamento; il presente regolamento è fondato sul meccanismo di coerenza del regolamento (UE) 2016/679. Gli Stati membri dovrebbero poter disporre di più di una autorità di controllo, al fine di rispecchiare la loro struttura costituzionale, organizzativa e amministrativa. Le autorità di controllo dovrebbero anche essere responsabili del monitoraggio dell'applicazione del presente regolamento per quanto riguarda i dati delle comunicazioni elettroniche per le entità giuridiche. Tali compiti supplementari non dovrebbero mettere a repentaglio la capacità delle autorità di controllo di espletare le proprie mansioni in merito alla tutela dei dati personali a norma del regolamento (UE) 2016/679 e del presente regolamento. Ogni autorità di controllo dovrebbe essere dotata delle risorse finanziarie e umane aggiuntive nonché delle strutture e delle infrastrutture necessarie all'esecuzione efficace delle sue mansioni nell'ambito del presente regolamento.

39) Ogni autorità di controllo dovrebbe avere la competenza, nel territorio del proprio Stato membro, a esercitare i poteri e ad assolvere i compiti a essa stabiliti dal presente regolamento. Al fine di garantire un monitoraggio e un'applicazione coerenti del presente regolamento in tutta l'Unione, le autorità di controllo dovrebbero avere gli stessi compiti e poteri effettivi in ciascuno Stato membro, fatti salvi i poteri delle autorità preposte all'esercizio dell'azione penale ai sensi del diritto degli Stati membri, il potere di intentare un'azione e di agire in sede giudiziale o stragiudiziale in caso di violazione del presente regolamento. Nell'applicare il presente regolamento gli Stati membri e le rispettive autorità di controllo sono invitati a considerare le esigenze specifiche delle micro, piccole e medie imprese.

40) Per rafforzare il rispetto delle norme del presente regolamento, ogni autorità di controllo dovrebbe avere il potere di imporre sanzioni anche amministrative pecuniarie in caso di violazione del regolamento, in aggiunta o in sostituzione di misure appropriate imposte dall'autorità di controllo ai sensi del presente regolamento. Il presente regolamento dovrebbe specificare le violazioni, indicare il limite massimo e i criteri per prevedere le relative sanzioni amministrative pecuniarie, che dovrebbero essere stabilite dall'autorità di controllo competente per ogni singolo caso, tenuto conto di tutte le circostanze pertinenti della situazione specifica, in particolare della natura, gravità e durata dell'infrazione e delle relative conseguenze, nonché delle misure adottate per assicurare la conformità agli obblighi derivanti dal presente regolamento e prevenire o attenuare le conseguenze della violazione. Per stabilire una sanzione amministrativa a norma del presente regolamento, un'impresa dovrebbe essere conforme a quanto disposto agli articoli 101 e 102 del trattato.

41) Al fine di conseguire gli obiettivi del regolamento, segnatamente tutelare i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali, e garantire la libera circolazione di tali dati nell'Unione, è opportuno delegare alla Commissione il potere di adottare atti conformemente all'articolo 290 del trattato onde integrare il presente regolamento. In particolare, gli atti delegati dovrebbero essere adottati in merito alle informazioni da comunicare, anche per mezzo

di icone normalizzate che diano una panoramica facilmente visibile e intelligibile della raccolta delle informazioni emesse dall'apparecchiatura terminale, la finalità, il responsabile e ogni eventuale misura pertinenti cui l'utente finale può ricorrere per minimizzare la raccolta. Gli atti delegati sono altresì necessari per precisare un codice identificativo delle chiamate a fini di commercializzazione diretta, comprese quelle effettuate per mezzo di sistemi automatici di chiamata e comunicazione. È di particolare importanza che la Commissione svolga adeguate consultazioni, nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016[8]. In particolare, al fine di garantire una partecipazione paritaria alla preparazione degli atti delegati, il Parlamento europeo e il Consiglio dovrebbero ricevere tutti i documenti contestualmente agli esperti degli Stati membri, e i loro esperti dovrebbero avere sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione incaricati della preparazione degli atti delegati. Al fine inoltre di garantire condizioni uniformi di esecuzione del presente regolamento, dovrebbero essere attribuite alla Commissione competenze di esecuzione ove previsto dal presente regolamento. È altresì opportuno che tali competenze siano esercitate conformemente al regolamento (UE) n. 182/2011.

42) Poiché l'obiettivo del presente regolamento, vale a dire garantire un livello equivalente di tutela delle persone fisiche e giuridiche nonché la libera circolazione delle comunicazioni elettroniche nell'Unione, non può essere conseguito in misura sufficiente dagli Stati membri ma, a motivo della portata e degli effetti dell'azione in questione, può essere conseguito meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. Il presente regolamento si limita a quanto è necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

43) È opportuno abrogare la direttiva 2002/58/CE,

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

[8] Accordo interistituzionale "Legiferare meglio" tra il Parlamento europeo, il Consiglio dell'Unione europea e la Commissione europea del 13 aprile 2016 (GU L 123 del 12.5.2016, pag. 1).

CAPO I
DISPOSIZIONI GENERALI

Articolo 1
Oggetto

1. Il presente regolamento stabilisce norme in materia di tutela dei diritti e delle libertà fondamentali delle persone fisiche e giuridiche per quanto attiene alla fornitura e all'uso di servizi di comunicazione elettronica, in particolare il diritto al rispetto della vita privata e delle comunicazioni nonché la tutela delle persone fisiche in merito al trattamento dei dati personali.

2. Il presente regolamento garantisce la libera circolazione dei dati delle comunicazioni elettroniche e dei servizi di comunicazione elettronica nell'Unione, i quali non sono limitati né proibiti per motivi connessi al rispetto della vita privata e delle comunicazioni delle persone fisiche e giuridiche nonché la tutela delle persone fisiche per quanto attiene al trattamento dei dati personali.

3. Quanto disposto dal presente regolamento precisa e integra il regolamento (UE) 2016/679 stabilendo norme specifiche ai fini di cui ai paragrafi 1 e 2.

Articolo 2
Ambito di applicazione materiale

1. Il presente regolamento si applica al trattamento dei dati delle comunicazioni elettroniche effettuato in relazione alla fornitura e alla fruizione dei servizi di comunicazione elettronica e alle informazioni connesse alle apparecchiature terminali degli utenti finali.

2. Il presente regolamento non si applica:

(a) alle attività che non rientrano nel campo di applicazione del diritto dell'Unione;

(b) alle attività degli Stati membri che rientrano nell'ambito di applicazione del titolo V, capo II, del trattato sull'Unione europea;

(c) ai servizi di comunicazione elettronica non accessibili al pubblico;

(d) alle attività delle 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;

3. Il trattamento dei dati delle comunicazioni elettroniche da parte delle istituzioni, degli organi e delle agenzie dell'Unione europea è disciplinato dal regolamento (UE) 00/0000 [nuovo regolamento che sostituisce il regolamento (CE) n. 45/2001].

4. Il presente regolamento non pregiudica pertanto l'applicazione della direttiva 2000/31/CE[9], in particolare delle norme relative alla responsabilità dei prestatori intermediari di servizi di cui agli articoli da 12 a 15 della medesima direttiva.

5. Il presente regolamento non pregiudica l'applicazione della direttiva 2014/53/UE.

[9] 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 L 178 del 17.7.2000, pag. 1).

Articolo 3
Ambito di applicazione e rappresentante territoriali

1. Il presente regolamento si applica:

(a) alla fornitura di servizi di comunicazione elettronica a utenti finali nell'Unione, indipendentemente dall'obbligo di pagamento da parte degli utenti finali;

(b) all'utilizzo di tali servizi;

(c) alla tutela delle informazioni connesse alle apparecchiature terminali degli utenti finali ubicati nell'Unione.

2. Qualora il fornitore di un servizio di comunicazione elettronica non sia ubicato nell'Unione, esso designa per iscritto un rappresentante nell'Unione.

3. Il rappresentante è stabilito in uno degli Stati membri in cui sono ubicati gli utenti finali di tali servizi di comunicazione elettronica.

4. Il rappresentante ha il potere di rispondere a domande e fornire informazioni oltre o in vece del fornitore rappresentato, in particolare alle autorità di controllo e agli utenti finali, in merito a tutte le questioni connesse al trattamento dei dati delle comunicazioni elettroniche al fine di garantire la conformità con il presente regolamento.

5. La designazione di un rappresentante a norma del paragrafo 2 lascia impregiudicate le azioni legali che potrebbero essere promosse contro una persona fisica o giuridica che effettua il trattamento dei dati delle comunicazioni elettroniche in relazione alla fornitura di servizi di comunicazione elettronica erogati al di fuori dell'Unione verso utenti finali ubicati nell'Unione.

Articolo 4
Definizioni

1. Ai fini del presente regolamento si applicano le seguenti definizioni:

(a) le definizioni contenute nel regolamento (UE) 2016/679;

(b) le definizioni di "rete di comunicazione elettronica", "servizio di comunicazione elettronica", "servizio di comunicazione interpersonale", "servizio di comunicazione interpersonale basato sul numero", "servizio di comunicazione interpersonale indipendente dal numero", "utente finale" e "chiamata" di cui rispettivamente all'articolo 2, punti 1), 4), 5), 6), 7), 14) e 21) della [direttiva che istituisce il codice europeo delle comunicazioni elettroniche];

(c) La definizione di "apparecchiatura terminale" di cui all'articolo 1, punto 1), della direttiva 2008/63/CE della Commissione[10].

2. Ai fini del paragrafo 1, lettera b), la definizione di "servizio di comunicazione interpersonale" comprende servizi che consentono la comunicazione interpersonale e interattiva come semplice caratteristica accessoria di importanza minore intrinsecamente connessa a un altro servizio.

3. Ai fini del presente regolamento si applicano inoltre le seguenti definizioni:

[10] Direttiva 2008/63/CE della Commissione, del 20 giugno 2008, relativa alla concorrenza sui mercati delle apparecchiature terminali di telecomunicazioni (GU L 162 del 21.6.2008, pag. 20).

(a) “dati delle comunicazioni elettroniche”, il contenuto e i metadati delle comunicazioni elettroniche;

(b) “contenuto delle comunicazioni elettroniche”, il contenuto scambiato attraverso servizi di comunicazione elettronica, quale testo, voce, video, immagini e suono;

(c) “metadati delle comunicazioni elettroniche”, i dati trattati in una rete di comunicazione elettronica per trasmettere, distribuire o scambiare il contenuto delle comunicazioni elettroniche compresi i dati usati per tracciare e identificare la fonte e il destinatario di una comunicazione, i dati relativi alla localizzazione del dispositivo generati nel contesto della fornitura di servizi di comunicazione elettronica nonché la data, l’ora, la durata e il tipo di comunicazione;

(d) “elenco pubblico”, elenco di utenti finali di servizi di comunicazione elettronica, in forma stampata o elettronica, pubblicato o a disposizione del pubblico o a una parte del pubblico, anche per mezzo di un servizio di consultazione elenchi;

(e) “posta elettronica”: messaggi contenenti testi, voci, video, suoni o immagini trasmessi attraverso una rete di comunicazione elettronica, che possono essere archiviati in rete, nelle risorse informatiche connesse o nell’apparecchiatura terminale ricevente;

(f) “comunicazioni di commercializzazione diretta”, qualsiasi forma di pubblicità, scritta od orale, inviata a uno o più utenti identificati o identificabili di servizi di comunicazione elettronica, anche mediante sistemi automatici di chiamata e comunicazione;

(g) “chiamate vocali a fini di commercializzazione diretta”, chiamate dal vivo che non contemplano il ricorso a sistemi automatici di chiamata e comunicazione;

(h) “sistemi automatici di chiamata e comunicazione”, sistemi in grado di avviare chiamate a uno o più destinatari conformemente alle istruzioni relative a detto sistema, e di trasmettere suoni non emessi dal vivo, comprese le chiamate effettuate mediante sistemi automatici di chiamata e comunicazione che collegano il chiamato a un operatore.

CAPO II
TUTELA DELLE COMUNICAZIONI ELETTRONICHE DELLE PERSONE FISICHE E GIURIDICHE NONCHÉ DELLE INFORMAZIONI CONSERVATE NELLE APPARECCHIATURE TERMINALI

Articolo 5
Riservatezza dei dati delle comunicazioni elettroniche

I dati delle comunicazioni elettroniche sono riservati. Sono vietate tutte le interferenze con i dati delle comunicazioni elettroniche, quali ascolto, registrazione, conservazione, monitoraggio, scansione o altri tipi di intercettazione, sorveglianza o trattamento dei dati delle comunicazioni elettroniche, da parte di persone diverse dagli utenti finali, salvo ove consentito dal presente regolamento.

Articolo 6

Trattamento consentito dei dati delle comunicazioni elettroniche

1. I fornitori di reti e servizi di comunicazione elettronica possono trattare i dati delle comunicazioni elettroniche se:

(a) necessario per realizzare la trasmissione della comunicazione, per la durata necessaria a tal fine, oppure

(b) se necessario per mantenere o ripristinare la sicurezza delle reti e dei servizi di comunicazione elettronica o rilevare problemi e/o errori tecnici nella trasmissione di comunicazioni elettroniche, per la durata necessaria a tal fine.

2. I fornitori di servizi di comunicazione elettronica possono trattare i metadati delle comunicazioni elettroniche se:

(a) necessario per soddisfare i requisiti di qualità obbligatori a norma della [direttiva che istituisce il codice europeo delle comunicazioni elettroniche] o del regolamento (UE) 2015/2120[11], per la durata necessaria a tal fine; oppure

(b) se necessario a fini di fatturazione, calcolo di pagamenti di interconnessione, rilevamento o arresto di un uso fraudolento o abusivo dei servizi di comunicazione elettronica o di abbonamento agli stessi; oppure

(c) se l'utente finale ha prestato il suo consenso al trattamento dei metadati delle sue comunicazioni per uno o più fini specificati, compresa l'erogazione di servizi di traffico a tali utenti finali, purché il o i fini in questione non possano essere realizzati mediante un trattamento anonimizzato delle informazioni.

3. I fornitori di servizi di comunicazione elettronica possono trattare il contenuto delle comunicazioni elettroniche solo:

(a) a fini di erogazione di un servizio specifico a un utente finale, se l'utente finale o gli utenti finali hanno prestato il loro consenso al trattamento del contenuto delle loro comunicazioni e l'erogazione del servizio non può essere realizzata senza il trattamento di tale contenuto; oppure

(b) se tutti gli utenti finali interessati hanno prestato il loro consenso al trattamento del contenuto delle loro comunicazioni elettroniche per uno o più fini specificati che non possono essere realizzati mediante il trattamento anonimizzato delle informazioni e il fornitore ha consultato l'autorità di controllo. Si applica l'articolo 36, punti 2) e 3), del regolamento (UE) 2016/679 alla consultazione dell'autorità di controllo.

Articolo 7

Conservazione e cancellazione dei dati delle comunicazioni elettroniche

1. Fatto salvo quanto disposto all'articolo 6, paragrafo 1, lettera b) e all'articolo 6, paragrafo 3, lettere a) e b), il fornitore del servizio di comunicazioni elettroniche cancella il contenuto delle comunicazioni elettroniche o anonimizza tali dati dopo

[11] Regolamento (UE) 2015/2120 del Parlamento europeo e del Consiglio, del 25 novembre 2015, che stabilisce misure riguardanti l'accesso a un'Internet aperta e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione (GU L 310 del 26.11.2015, pag. 1).

che il o i destinatari previsti hanno ricevuto il contenuto della comunicazione elettronica. Tali dati possono essere registrati o conservati dagli utenti finali o da un terzo da essi incaricato di registrare, conservare o trattare altrimenti tali dati, a norma del regolamento (UE) 2016/679.

2. Fatto salvo quanto disposto all'articolo 6, paragrafo 1, lettera b) e all'articolo 6, paragrafo 2, lettere a) e c), il fornitore del servizio di comunicazioni elettroniche cancella i metadati delle comunicazioni elettroniche o anonimizza tali dati quando non sono più necessari al fine di trasmettere una comunicazione.

3. Se il trattamento dei metadati delle comunicazioni elettroniche avviene a fini di fatturazione, a norma dell'articolo 6, paragrafo 2, lettera b), i pertinenti metadati possono essere conservati fino alla fine del periodo nel quale una fattura può essere legalmente contestata o un pagamento può essere preteso, conformemente al diritto nazionale.

Articolo 8

Tutela delle informazioni conservate nell'apparecchiatura terminale relative agli utenti finali

1. L'uso delle capacità di trattamento e conservazione dell'apparecchiatura terminale e la raccolta di informazioni dall'apparecchiatura terminale degli utenti finali, comprese informazioni relative ai programmi e i componenti, da parte di una parte diversa dall'utente finale, è proibita, eccetto per i seguenti motivi:

(a) se necessario al solo fine di effettuare la trasmissione di una comunicazione elettronica su una rete di comunicazione elettronica; oppure

(b) se l'utente finale ha prestato il suo consenso; oppure

(c) se necessario per erogare un servizio della società dell'informazione richiesto dall'utente finale; oppure

(d) se necessario per misurare il pubblico del web, purché tale misurazione sia effettuata dal fornitore del servizio della società dell'informazione richiesto dall'utente finale.

2. La raccolta delle informazioni emesse dall'apparecchiatura terminale per consentirne la connessione a un altro dispositivo o a un'apparecchiatura di rete è proibita, eccetto se:

(a) effettuata esclusivamente al fine di e per il tempo necessario a stabilire una connessione; oppure

(b) se è visualizzato un avviso chiaro e ben visibile, inteso a informare almeno delle modalità, delle finalità, del responsabile e di ogni altra informazione richiesta a norma dell'articolo 13 del regolamento (UE) 679/2016, della raccolta di dati personali nonché di ogni misura a disposizione dell'utente finale dell'apparecchiatura terminale per arrestare o minimizzare tale raccolta.

La raccolta di tali informazioni è subordinata all'applicazione di opportune misure tecniche e organizzative per garantire un livello di sicurezza proporzionato ai rischi, conformemente a quanto disposto all'articolo 32 del regolamento (UE) 2016/679.

3. Le informazioni da comunicare agli interessati a norma del paragrafo 2, lettera b), possono essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme della raccolta.

4. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 27 al fine di stabilire le informazioni da comunicare sotto forma di icona e le procedure per fornire icone standardizzate.

Articolo 9
Consenso

1. Si applica la definizione di consenso e le relative condizioni di cui all'articolo 4, paragrafo 11, e all'articolo 7, del regolamento (UE) 2016/679.

2. Fatto salvo quanto disposto dal paragrafo 1, laddove tecnicamente possibile e praticabile, ai fini dell'articolo 8, paragrafo 1, lettera b), il consenso può essere espresso mediante le opportune impostazioni di un'applicazione informatica che consente l'accesso a internet.

3. Gli utenti finali che hanno acconsentito al trattamento dei dati delle comunicazioni elettroniche a norma dell'articolo 6, paragrafo 2, lettera c), e dell'articolo 6, paragrafo 3, lettere a) e b), dispongono della facoltà di revocare tale consenso in qualsiasi momento, conformemente a quanto disposto all'articolo 7, paragrafo 3, del regolamento (UE) 2016/679, e ogni sei mesi viene loro rammentata tale possibilità, finché prosegue il trattamento.

Articolo 10
Informazioni e opzioni da fornire per le impostazioni relative alla vita privata

1. I programmi immessi sul mercato che consentono le comunicazioni elettroniche, compreso il recupero e la presentazione di informazioni in rete, offrono l'opzione di impedire che terzi conservino informazioni sull'apparecchiatura terminale di un utente finale o trattino le informazioni già conservate su detta apparecchiatura.

2. All'installazione il programma informa l'utente finale delle impostazioni relative alla vita privata e per proseguire nell'installazione richiede il consenso dell'utente per una data impostazione.

3. Qualora un programma sia già installato al 25 maggio 2018, i requisiti di cui ai paragrafi 1 e 2 sono soddisfatti al momento del primo aggiornamento del programma e comunque non oltre il 25 agosto 2018.

Articolo 11
Restrizioni

1. Il diritto dell'Unione o dello Stato membro può limitare per mezzo di una misura legislativa l'ambito di applicazione degli obblighi e dei diritti di cui agli articoli da 5 a 8 se siffatta limitazione rispetta l'essenza dei diritti e delle libertà fondamentali e costituisce una misura necessaria, appropriata e proporzionata in una società democratica intesa a salvaguardare uno o più interessi pubblici ai sensi dell'articolo 23, paragrafo 1, lettere da a) a e), del regolamento (UE) 2016/679 o un monitoraggio, un'ispezione o una funzione regolamentare in relazione all'esercizio dell'autorità ufficiale per tali interessi.

2. I fornitori di servizi di comunicazione elettronica adottano procedure interne intese a rispondere alle richieste di accesso ai dati delle comunicazioni elettroniche degli utenti finali in base a una misura legislativa adottata ai sensi del paragrafo 1. Su richiesta forniscono alla competente autorità di controllo informazioni su dette

procedure, sul numero di richieste ricevute, sui motivi legali addotti e sulla loro risposta.

CAPO III
DIRITTI DELLE PERSONE FISICHE E GIURIDICHE DI CONTROLLARE LE COMUNICAZIONI ELETTRONICHE

Articolo 12
Presentazione e restrizione dell'identificazione della linea chiamante e collegata

1. Qualora sia prevista la presentazione della linea chiamante e connessa a norma dell'articolo [107] della [direttiva che istituisce il codice europeo delle comunicazioni elettroniche], i fornitori di servizi di comunicazione interpersonale basata sul numero accessibili al pubblico comunicano quanto segue:

(a) la possibilità per l'utente finale chiamante di impedire la presentazione dell'identificazione della linea chiamante per ogni singola chiamata, per connessione o su base permanente;

(b) la possibilità per l'utente finale chiamato di impedire la presentazione dell'identificazione della linea chiamante per le chiamate in entrata;

(c) la possibilità per l'utente finale chiamato di rifiutare le chiamate in entrata se la presentazione dell'identificazione della linea chiamante è stata bloccata dall'utente finale chiamante;

(d) la possibilità per l'utente finale chiamato di impedire la presentazione dell'identificativo della linea connessa all'utente finale chiamante.

2. Le possibilità di cui al paragrafo 1, lettere a), b), c) e d) sono messe a disposizione degli utenti finali in modo semplice e a titolo gratuito.

3. Il paragrafo 1, lettera a), si applica anche alle chiamate provenienti dall'Unione e dirette verso paesi terzi. Il paragrafo 1, lettere b), c) e d), si applica anche alle chiamate in entrata provenienti da paesi terzi.

4. Qualora sia offerta la presentazione della linea chiamante o l'identificazione della linea connessa, i fornitori di servizi di comunicazione interpersonale basata sul numero accessibili al pubblico comunicano al pubblico le informazioni in merito alle opzioni di cui al paragrafo 1, lettere a), b), c) e d).

Articolo 13
Eccezioni alla presentazione e restrizione dell'identificazione della linea chiamante e collegata

1. Indipendentemente dal fatto che l'utente finale chiamante abbia impedito la presentazione dell'identificazione, nei casi di chiamate a servizi di emergenza i fornitori di servizi di comunicazione interpersonale basata sul numero accessibili al pubblico annullano la soppressione della presentazione dell'identificazione della linea chiamante e il rifiuto o il mancato consenso di un utente finale per il trattamento dei metadati, linea per linea per le organizzazioni che fruiscono delle comunicazioni di emergenza, compresi i punti di risposta di pubblica sicurezza, al fine di rispondere a tali comunicazioni.

2. Gli Stati membri adottano disposizioni più specifiche per quanto attiene all'istituzione di procedure e alle circostanze in cui i fornitori di servizi di comunicazione interpersonale basata sul numero accessibili al pubblico possono superare la soppressione della presentazione dell'identificazione della linea chiamante su base temporanea, quando gli utenti finali richiedono il tracciamento di chiamate maligne o importune.

Articolo 14
Blocco delle chiamate in entrata

I fornitori di servizi di comunicazione interpersonale basata sul numero accessibili al pubblico adottano misure all'avanguardia affinché gli utenti finali possano limitare il ricevimento di chiamate indesiderate e forniscono inoltre all'utente finale chiamato le seguenti possibilità, a titolo gratuito:

(a) bloccare le chiamate in entrata provenienti da numeri specifici o da fonti anonime;

(b) porre termine alla trasmissione delle chiamate automatiche effettuate da terzi verso l'apparecchiatura terminale dell'utente finale.

Articolo 15
Elenchi pubblici

1. I fornitori di elenchi pubblici ottengono il consenso degli utenti finali aventi natura di persone fisiche per inserire i loro dati personali nell'elenco e quindi ottengono il consenso da tali utenti finali per l'inserimento dei dati per categorie di dati personali nella misura in cui tali dati sono pertinenti al fine perseguito dall'elenco quale determinato dal fornitore del servizio. I fornitori conferiscono a tali utenti finali aventi natura di persone fisiche i mezzi per accertare, rettificare e cancellare tali dati.

2. I fornitori di elenchi pubblici comunicano agli utenti finali aventi natura di persone fisiche e i cui dati sono presenti nell'elenco, le funzioni di ricerca disponibili dell'elenco e ottengono il consenso degli utenti finali prima di abilitare tali funzioni di ricerca connesse ai loro propri dati.

3. I fornitori di elenchi pubblici prevedono che gli utenti finali aventi natura di persone giuridiche abbiano la possibilità di contestare l'inserimento nell'elenco dei dati a esse relativi. I fornitori conferiscono a tali utenti finali aventi natura di persone giuridiche i mezzi per accertare, rettificare e cancellare tali dati.

4. La possibilità che gli utenti finali non siano inclusi in un elenco pubblico o di accertare, rettificare e cancellare tutti i dati a essi connessi è offerta a titolo gratuito.

Articolo 16
Comunicazioni indesiderate

1. Le persone fisiche o giuridiche possono avvalersi dei servizi di comunicazione elettronica al fine di inviare comunicazioni di commercializzazione diretta a utenti finali aventi natura di persone fisiche che hanno espresso il loro consenso.

2. Allorché una persona fisica o giuridica ottiene dai suoi clienti le coordinate elettroniche per la posta elettronica nel contesto della vendita di un prodotto o servizio ai sensi del regolamento (UE) 2016/679, la medesima persona fisica o giuridica può utilizzare tali coordinate elettroniche a scopi di commercializzazione

diretta di propri prodotti o servizi analoghi, solamente se ai clienti è offerta in modo chiaro e distinto la possibilità di opporsi gratuitamente e agevolmente a tale uso. Il diritto di obiezione è dato al momento della raccolta e ogniqualvolta si invii un messaggio.

3. Fatto salvo quanto disposto ai paragrafi 1 e 2, le persone fisiche o giuridiche che usano servizi di comunicazione elettronica per effettuare chiamate di commercializzazione diretta:

(a) presentano l'identità di una linea alla quale possono essere contattati; oppure

(b) presentano un codice o prefisso specifico che identifichi il fatto che trattasi di chiamata a fini commerciali.

4. Fatto salvo quanto disposto al paragrafo 1, gli Stati membri possono stabilire per legge che l'effettuazione di chiamate di commercializzazione diretta vocali verso utenti finali aventi natura di persone fisiche è consentita solo nel rispetto degli utenti finali che sono persone naturali che non hanno espresso la loro obiezione a ricevere tali comunicazioni.

5. Gli Stati membri garantiscono inoltre, nel quadro del diritto dell'Unione e della normativa nazionale applicabile, un'adeguata tutela degli interessi legittimi degli utenti finali aventi natura di persone fisiche relativamente alle comunicazioni indesiderate inviate con i mezzi di cui al paragrafo 1.

6. Le persone fisiche o giuridiche che si avvalgono di servizi di comunicazione per trasmettere comunicazioni di commercializzazione diretta informano gli utenti finali della natura commerciale della comunicazione e dell'identità della persona giuridica o fisica per conto della quale è trasmessa la comunicazione e forniscono ai destinatari le informazioni necessarie affinché possano esercitare agevolmente il loro diritto di revoca del consenso a ricevere ulteriori messaggi commerciali.

7. Alla Commissione è conferito il potere di adottare misure di attuazione a norma dell'articolo 26, paragrafo 2, specificando il codice/prefisso inteso a identificare le chiamate commerciali, a norma del paragrafo 3, lettera b).

Articolo 17
Informazioni sui rischi relativi alla sicurezza rilevati

Nel caso in cui esista un particolare rischio di compromettere la sicurezza delle reti e dei servizi di comunicazione elettronica, il fornitore di un servizio di comunicazione elettronica ne informa gli utenti finali e, qualora il rischio sia al di fuori del campo di applicazione delle misure che devono essere prese dal fornitore di servizio, comunica agli utenti finali tutti i possibili rimedi, compresi i relativi costi presumibili.

CAPO IV
AUTORITÀ DI CONTROLLO E APPLICAZIONE INDIPENDENTI

Articolo 18
Autorità di controllo indipendenti

1. La o le autorità di controllo indipendenti responsabili di monitorare l'applicazione del regolamento (UE) 2016/679 sono altresì responsabili di monitorare l'applicazione

del presente regolamento. I capi VI e VII del regolamento (CE) n. 2016/679 si applicano *mutatis mutandis*. Le mansioni e i poteri delle autorità di controllo sono espletati nei confronti degli utenti finali.

2. La o le autorità di controllo di cui al paragrafo 1 collaborano qualora opportuno con le autorità nazionali di regolamentazione istituite a norma della [direttiva che istituisce il codice europeo delle comunicazioni elettroniche].

Articolo 19
Comitato europeo per la protezione dei dati

Il comitato europeo per la protezione dei dati istituito dall'articolo 68 del regolamento (UE) 2016/679 è competente per garantire un'applicazione coerente del presente regolamento. A tal fine il comitato europeo per la protezione dei dati espleta le mansioni di cui all'articolo 70 del regolamento (UE) 2016/679. Il comitato svolge inoltre i seguenti compiti:

(a) fornisce consulenza alla Commissione in merito a qualsiasi proposta di modifica del presente regolamento;

(b) esamina, di propria iniziativa o su richiesta di uno dei suoi membri o della Commissione, qualsiasi questione relativa all'applicazione del presente regolamento e pubblica linee guida, raccomandazioni e migliori pratiche al fine di promuovere l'applicazione coerente del presente regolamento.

Articolo 20
Procedure di cooperazione e coerenza

Ogni autorità di controllo contribuisce a un'applicazione coerente del presente regolamento in tutta l'Unione. A tal fine le autorità di controllo collaborano fra loro e con la Commissione a norma del capo VII del regolamento (UE) 2016/679 in relazione alle materie disciplinate dal presente regolamento.

CAPO V
RICORSI, RESPONSABILITÀ E SANZIONI

Articolo 21
Ricorsi

1. Fatto salvo ogni altro rimedio amministrativo o giudiziario, tutti gli utenti finali dei servizi di comunicazione elettronica dispongono degli stessi rimedi di cui agli articoli 77, 78 e 79 del regolamento (UE) 2016/679.

2. Tutte le persone fisiche o giuridiche diverse dagli utenti finali i cui interessi sono lesi dalle violazioni del presente regolamento e aventi un interesse legittimo nella cessazione o nella proibizione delle presunte violazioni, compreso un fornitore di servizi di comunicazione che protegga i propri interessi commerciali legittimi, hanno il diritto di intentare un'azione legale contro tali violazioni.

Articolo 22
Diritto al risarcimento e responsabilità

Tutti gli utenti finali dei servizi di comunicazione elettronica che hanno subito un danno materiale o immateriale in conseguenza di una violazione del presente regolamento, hanno il

diritto di ricevere un risarcimento da parte del responsabile della violazione per il danno subito, se dimostrano che l'evento dannoso non è loro in alcun modo imputabile, a norma dell'articolo 82 del regolamento (UE) 2016/679.

Articolo 23
Condizioni generali per imporre sanzioni amministrative pecuniarie

1. Ai fini del presente articolo, il capo VII del regolamento (UE) 2016/679 si applica alle violazioni del presente regolamento.

2. In conformità al paragrafo 1, la violazione delle seguenti disposizioni del presente regolamento è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 EUR, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

(a) gli obblighi di tutte le persone fisiche o giuridiche che effettuano il trattamento dei dati delle comunicazioni elettroniche a norma dell'articolo 8;

(b) gli obblighi dei fornitori di programmi che consentono le comunicazioni elettroniche, a norma dell'articolo 10;

(c) gli obblighi dei fornitori di elenchi pubblici a norma dell'articolo 15;

(d) gli obblighi di tutte le persone fisiche o giuridiche che si avvalgono del servizio di comunicazione elettronica a norma dell'articolo 16.

3. Le violazioni del principio della riservatezza delle comunicazioni, del trattamento consentito dei dati delle comunicazioni elettroniche, dei termini ultimi previsti per la cancellazione in conformità degli articoli 5, 6 e 7, a norma del paragrafo 1, sono soggette a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

4. Gli Stati membri stabiliscono le norme relative alle sanzioni per le violazioni degli articoli 12, 13, 14 e 17.

5. In conformità del paragrafo 18, l'inosservanza di un ordine da parte di un'autorità di controllo è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

6. Fatti salvi i poteri correttivi delle autorità di controllo a norma dell'articolo 18, ogni Stato membro può prevedere norme che dispongono se e in quale misura possano essere imposte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro.

7. L'esercizio da parte dell'autorità di controllo dei poteri attribuitile dal presente articolo è soggetto a garanzie procedurali adeguate in conformità del diritto dell'Unione e degli Stati membri, inclusi il ricorso giurisdizionale effettivo e il giusto processo.

8. Se l'ordinamento giuridico dello Stato membro non prevede sanzioni amministrative pecuniarie, il presente articolo può essere applicato in maniera tale che l'azione sanzionatoria sia avviata dall'autorità di controllo competente e la sanzione pecuniaria sia imposta dalle competenti autorità giurisdizionali nazionali, garantendo nel contempo che i mezzi di ricorso siano effettivi e abbiano effetto equivalente alle sanzioni amministrative pecuniarie imposte dalle autorità di controllo. In ogni caso,

le sanzioni pecuniarie imposte devono essere effettive, proporzionate e dissuasive. Tali Stati membri notificano alla Commissione le disposizioni di legge adottate a norma del presente paragrafo al più tardi entro il [xxx] e comunicano sollecitamente ogni successiva modifica.

Articolo 24
Sanzioni

1. Gli Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del presente regolamento, in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 23, e adottano tutti i provvedimenti necessari per assicurarne l'applicazione. Tali sanzioni devono essere effettive, proporzionate e dissuasive.

2. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 1 entro 18 mesi dalla data di cui all'articolo 29, paragrafo 2, e comunica sollecitamente ogni successiva modifica.

CAPO VI
ATTI DELEGATI E ATTI DI ESECUZIONE

Articolo 25
Esercizio della delega

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.

2. Il potere di adottare atti delegati di cui all'articolo 8, paragrafo 4, è conferito alla Commissione per un periodo di tempo indeterminato a decorrere dalla [data di entrata in vigore del presente regolamento].

3. La delega di potere di cui all'articolo 8, paragrafo 4, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella Gazzetta ufficiale dell'Unione europea o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.

4. Prima di adottare un atto delegato, la Commissione consulta gli esperti designati da ciascuno Stato membro conformemente ai principi stabiliti dall'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016.

5. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.

6. L'atto delegato adottato ai sensi dell'articolo 8, paragrafo 4, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di due mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo, sia il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di due mesi su iniziativa del Parlamento europeo o del Consiglio.

Articolo 26
Comitato

1. La Commissione è assistita dal comitato per le comunicazioni istituito all'articolo 110 della [direttiva che istituisce il codice europeo delle comunicazioni elettroniche]. Detto comitato è un comitato ai sensi del regolamento (UE) n. 182/2011[12].

2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5 del regolamento (UE) n. 182/2011.

CAPO VII
DISPOSIZIONI FINALI

Articolo 27
Abrogazione

1. La direttiva 2002/58/CE è abrogata a decorrere dal 25 maggio 2018.

2. I riferimenti alla direttiva abrogata si intendono fatti al presente regolamento.

Articolo 28
Clausola di monitoraggio e valutazione

Entro il 1° gennaio 2018 la Commissione stila un programma particolareggiato per il monitoraggio dell'efficacia del presente regolamento.

Non oltre tre anni dalla data di applicazione del presente regolamento e successivamente ogni tre anni, la Commissione effettua una valutazione del presente regolamento e ne presenta i risultati salienti al Parlamento europeo, al Consiglio e al Comitato economico e sociale europeo. Se del caso la valutazione proporrà di modificare o abrogare il presente regolamento alla luce degli sviluppi giuridici, tecnici o economici.

Articolo 29
Entrata in vigore e applicazione

1. Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

2. Esso si applica a decorrere dal 25 maggio 2018.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

[12] Regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione (GU L 55 del 28.2.2011, pag. 13).

Fatto a Bruxelles, il

Per il Parlamento europeo
Il presidente

Per il Consiglio
Il presidente