



17/IT

WP 247

**Parere 1/2017 relativo  
alla proposta di regolamento sulla vita privata e le comunicazioni elettroniche  
(2002/58/CE)**

**adottato il 4 aprile 2017**

Il Gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. È l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE.

Le funzioni di segreteria sono espletate dalla direzione C (Diritti fondamentali e Stato di diritto) della Commissione europea, direzione generale Giustizia e consumatori, B-1049 Bruxelles, Belgio, Ufficio MO-59 05/035.

Sito Internet: [http://ec.europa.eu/justice/data-protection/index\\_en.htm](http://ec.europa.eu/justice/data-protection/index_en.htm)

**IL GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI**

istituito ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995,

visti gli articoli 29 e 30 della stessa,

visto il suo regolamento interno,

**HA ADOTTATO IL PRESENTE PARERE:**

## SINTESI

Il Gruppo di lavoro accoglie con favore la proposta della Commissione europea del 10 gennaio 2017 concernente un regolamento sulla vita privata e le comunicazioni elettroniche. In particolare, il Gruppo apprezza **la scelta del regolamento** come strumento normativo, in quanto assicura norme uniformi in tutta l'UE, garantisce chiarezza tanto alle autorità di controllo quanto alle organizzazioni e contribuisce ad assicurare la coerenza con il regolamento generale sulla protezione dei dati. Tale coerenza è ulteriormente favorita dalla decisione che **l'autorità competente per il monitoraggio del rispetto del regolamento generale sulla protezione dei dati** sia responsabile anche di assicurare l'applicazione delle norme in materia di vita privata e comunicazioni elettroniche.

Allo stesso tempo, la scelta di (mantenere) uno **strumento giuridico complementare** è positiva. La protezione delle comunicazioni riservate e delle apparecchiature terminali presenta caratteristiche specifiche che non sono affrontate dal regolamento generale sulla protezione dei dati. Di conseguenza, per assicurare un'adeguata tutela del diritto fondamentale al rispetto della vita privata e alla riservatezza delle comunicazioni, ivi inclusa la riservatezza delle apparecchiature terminali, sono necessarie disposizioni complementari sui servizi di questo tipo. A questo proposito, il Gruppo di lavoro sostiene fermamente **l'approccio basato su principi** seguito nel proposto regolamento, che stabilisce **divieti di ampia portata ed eccezioni di portata limitata**, nonché **l'applicazione mirata della nozione di consenso**.

Il Gruppo di lavoro accoglie con favore l'espansione dell'ambito di applicazione del proposto regolamento **ai fornitori di servizi over-the-top (OTT)**, ossia servizi che sono equivalenti sotto il profilo funzionale a mezzi di comunicazione più tradizionali e presentano quindi potenziali ripercussioni analoghe sulla vita privata e sul diritto alla segretezza delle comunicazioni delle persone nell'UE. Altrettanto positivo è il fatto che il proposto regolamento tratti in maniera chiara i **contenuti e i metadati associati** e riconosca che **i metadati possono rivelare dati estremamente sensibili**.

Tuttavia, il Gruppo di lavoro rileva anche quattro aspetti che destano **grave preoccupazione**. In relazione al **tracciamento dell'ubicazione delle apparecchiature terminali, alle condizioni che consentono l'analisi dei contenuti e dei metadati, alle impostazioni predefinite delle apparecchiature terminali e dei programmi e alle barriere di tracciamento (tracking wall)** il proposto regolamento riduce il livello di protezione garantito dal regolamento generale sulla protezione dei dati. Nel presente parere il Gruppo di lavoro fornisce suggerimenti specifici affinché il regolamento sulla vita privata e le comunicazioni elettroniche assicuri un pari o maggiore livello di protezione adeguato in considerazione della natura sensibile dei dati delle comunicazioni (in termini tanto di contenuti quanto di metadati).

Per quanto concerne il **tracciamento WiFi**, a seconda delle circostanze e delle finalità della raccolta dei dati, a norma del regolamento generale sulla protezione dei dati è probabile che tale tracciamento sia soggetto al consenso o possa essere effettuato soltanto se i dati personali raccolti vengono anonimizzati. In quest'ultimo caso è necessario che siano soddisfatte le seguenti quattro condizioni: la finalità della raccolta dei dati da un'apparecchiatura terminale è limitata a un mero conteggio statistico; il tracciamento è limitato nel tempo e nello spazio allo stretto necessario al raggiungimento di tale finalità; i dati saranno cancellati o anonimizzati

immediatamente dopo; sussistono possibilità effettive di esclusione (*opt-out*). La Commissione europea è invitata a promuovere una norma tecnica che preveda che i dispositivi mobili segnalino automaticamente un'eventuale obiezione al tracciamento.

In merito all'**analisi dei contenuti e dei metadati**, il punto di partenza dovrebbe essere il divieto di trattare dati delle comunicazioni in assenza del consenso di tutti gli utenti finali (mittenti e destinatari). Al fine di consentire ai fornitori di erogare servizi esplicitamente richiesti dall'utente, come ad esempio la funzionalità di ricerca e indicizzazione o servizi da testo a voce (*text-to-speech*), dovrebbe esistere un'eccezione nazionale per il trattamento di contenuti e metadati per finalità meramente personali dell'utente stesso.

In merito al **consenso al tracciamento**, il Gruppo di lavoro chiede un divieto esplicito alle barriere di tracciamento, ossia l'imposizione di scelte del tipo "prendere o lasciare" che formino gli utenti ad acconsentire al tracciamento per accedere a un servizio specifico.

Da ultimo, ma non meno importante, il Gruppo di lavoro raccomanda che le apparecchiature terminali e i programmi offrano, **per impostazione predefinita, impostazioni che proteggano la vita privata** e opzioni chiare per gli utenti per confermare o modificare tali impostazioni predefinite durante l'installazione. Le impostazioni devono essere facilmente accessibili durante l'uso. Gli utenti devono poter segnalare un consenso specifico tramite le impostazioni del navigatore. Le preferenze relative alla vita privata non dovrebbero essere limitate alle interferenze di terzi o ai marcatori (*cookie*). Il Gruppo di lavoro raccomanda vivamente di rendere obbligatoria l'adesione alla norma "*Do Not Track*" (che prevede il non tracciamento).

Il Gruppo ha individuato anche altri aspetti che destano preoccupazione, riguardanti ad esempio l'ambito di applicazione, la protezione delle apparecchiature terminali e la commercializzazione diretta, e questioni che meritano chiarimenti per proteggere meglio gli utenti finali e offrire maggiore certezza del diritto per tutte le parti interessate coinvolte.

## INDICE

<b>1. INTRODUZIONE .....</b>	<b>6</b>
<b>2. ASPETTI POSITIVI DEL REGOLAMENTO PROPOSTO .....</b>	<b>6</b>
<i>Armonizzazione a livello UE, allineamento delle sanzioni pecuniarie e applicazione esclusiva da parte delle autorità di protezione dei dati .....</i>	<i>6</i>
<i>Estensione dell'ambito di applicazione rispetto alla direttiva relativa alla vita privata e alle comunicazioni elettroniche .....</i>	<i>8</i>
<i>Applicazione mirata del concetto di consenso.....</i>	<i>11</i>
<b>3. ASPETTI DI GRAVE PREOCCUPAZIONE.....</b>	<b>11</b>
<i>La tutela garantita dal regolamento generale sulla protezione dei dati viene compromessa dal regolamento proposto.....</i>	<i>11</i>
<b>4. ALTRI ASPETTI CHE DESTANO PREOCCUPAZIONE .....</b>	<b>19</b>
<i>Occorre ampliare l'ambito di applicazione territoriale e materiale.....</i>	<i>19</i>
<i>È necessario rafforzare la protezione delle apparecchiature terminali .....</i>	<i>20</i>
<i>Commercializzazione diretta .....</i>	<i>24</i>
<i>Calendario.....</i>	<i>27</i>
<i>Ulteriori preoccupazioni .....</i>	<i>28</i>
<b>5. SUGGERIMENTI PER CHIARIMENTI AL FINE DI GARANTIRE LA CERTEZZA DEL DIRITTO .....</b>	<b>31</b>
<i>Chiarimenti in merito all'ambito di applicazione .....</i>	<i>31</i>
<i>Chiarimenti sul concetto di consenso e sulla sua applicazione .....</i>	<i>34</i>
<i>Chiarimenti sull'ubicazione e su altri metadati .....</i>	<i>36</i>
<i>Chiarimenti sulle comunicazioni indesiderate.....</i>	<i>37</i>
<i>Chiarimenti sull'applicazione di strumenti in materia di diritti fondamentali .....</i>	<i>39</i>
<i>Altri chiarimenti .....</i>	<i>40</i>

## 1. INTRODUZIONE

1. Il Gruppo di lavoro articolo 29 sulla protezione dei dati (in appresso: Gruppo di lavoro o Gruppo) accoglie con favore la proposta della Commissione europea (CE) relativa al regolamento sulla vita privata e le comunicazioni elettroniche (in appresso: la "proposta di regolamento", il "proposto regolamento/regolamento proposto" o il "regolamento sulla vita privata e le comunicazioni elettroniche")<sup>1</sup>, che intende sostituire la direttiva relativa alla vita privata e alle comunicazioni elettroniche<sup>2</sup>.
2. Molti aspetti del regolamento proposto sono positivi e con la sua presentazione la Commissione europea ha compiuto un passo importante. Tuttavia, il regolamento proposto può essere ulteriormente migliorato, non soltanto per proteggere meglio gli utenti finali, ma anche per introdurre una maggiore certezza del diritto per tutte le parti interessate coinvolte.
3. Il Gruppo di lavoro ha pertanto rilevato diversi aspetti che destano preoccupazione e formulato raccomandazioni per chiarimenti che dovrebbero essere presi in considerazione dal Parlamento europeo e dal Consiglio dei ministri nelle discussioni sulla proposta di regolamento. Il presente parere esporrà innanzitutto gli aspetti positivi del proposto regolamento, evidenziando successivamente le questioni che destano preoccupazione e i punti che richiedono chiarimenti.

## 2. ASPETTI POSITIVI DEL REGOLAMENTO PROPOSTO

*ARMONIZZAZIONE A LIVELLO UE, ALLINEAMENTO DELLE SANZIONI PECUNIARIE E APPLICAZIONE ESCLUSIVA DA PARTE DELLE AUTORITÀ DI PROTEZIONE DEI DATI*

4. Il Gruppo di lavoro accoglie con favore **la scelta del regolamento** come strumento normativo, in quanto ciò assicura che le norme siano uniformi in tutta l'UE (con talune eccezioni che saranno discusse in seguito) e garantisce chiarezza tanto alle autorità di controllo quanto alle organizzazioni. Inoltre, dato il ruolo chiave svolto dal regolamento generale sulla protezione dei dati<sup>3</sup> nel contesto del regolamento proposto, la scelta del regolamento contribuisce a garantire coerenza tra i due

---

<sup>1</sup> 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), 2017/0003 (COD), URL: <http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52017PC0010&from=IT>.

<sup>2</sup> 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), URL: <http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:32002L0058>.

<sup>3</sup> 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), URL: <http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016R0679>.

strumenti. Allo stesso tempo, **la scelta di (mantenere) uno strumento giuridico complementare** è positiva. La protezione delle comunicazioni riservate e delle apparecchiature terminali presenta caratteristiche specifiche che non sono affrontate dal regolamento generale sulla protezione dei dati. Di conseguenza, per assicurare un'adeguata tutela di questo diritto fondamentale, sono necessarie disposizioni complementari sui servizi di questo tipo. In questo contesto il Gruppo di lavoro **sostiene altresì l'approccio basato su principi, seguito nel regolamento proposto, che prevede l'adozione di divieti di ampia portata ed eccezioni di portata limitata**, e ritiene che si debba evitare l'introduzione di eccezioni aperte in linea con l'articolo 6 del regolamento generale sulla protezione dei dati, in particolare con l'articolo 6, lettera f, di tale regolamento (interesse legittimo).

5. **L'applicazione di tali norme da parte della stessa autorità responsabile del monitoraggio del rispetto del regolamento generale sulla protezione dei dati** sosterrà ulteriormente la coerenza tra i due strumenti. Data la relazione che intercorre tra la protezione dei dati personali e la protezione della riservatezza delle comunicazioni e delle apparecchiature terminali, è utile che l'applicazione delle disposizioni di cui al regolamento proposto sia affidata alla medesima autorità di controllo incaricata dell'applicazione del regolamento generale sulla protezione dei dati (considerando 38 e articolo 18 del regolamento proposto). Inoltre, la giurisprudenza della Corte di giustizia dell'Unione europea (CGUE)<sup>4</sup> conferma che è essenziale che l'autorità di controllo sia indipendente, come previsto dall'articolo 7 della Carta dei diritti fondamentali dell'Unione europea (in appresso: "Carta"). Nella pratica, tuttavia, ciò porterebbe a un notevole lavoro supplementare per le autorità di protezione dei dati, senza alcuna garanzia di adempimento in assenza di ottenimento di un bilancio supplementare. Di conseguenza, le autorità di protezione dei dati accolgono con favore il considerando 38 del regolamento proposto che sottolinea che 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. Inoltre accoglie altrettanto favorevolmente l'articolo 18, paragrafo 2, che stabilisce la base giuridica per la cooperazione tra le autorità di controllo del regolamento proposto e le autorità nazionali di regolamentazione della proposta direttiva che istituisce il codice europeo delle comunicazioni elettroniche<sup>5</sup>.
6. Data la stretta relazione tra il proposto regolamento e il regolamento generale sulla protezione dei dati, **l'allineamento delle sanzioni pecuniarie a norma del regolamento proposto rispetto a detto regolamento generale** è anch'esso un aspetto accolto con favore. Le attività che rientrano nell'ambito di applicazione del proposto regolamento sono molto sensibili, in quanto coinvolgono, tra l'altro, l'interferenza con le comunicazioni riservate e le apparecchiature terminali. Il livello

---

<sup>4</sup> Cfr. ad esempio sentenza della Corte del 6 ottobre 2015, C-362/14 (*Approdo sicuro*), punto 41 e sentenza della Corte del 21 dicembre 2016, C-203/15 e C-698/15 (*Tele2/Watson*), punto 123.

<sup>5</sup> Proposta di direttiva del Parlamento europeo e del Consiglio che istituisce il codice europeo delle comunicazioni elettroniche (rifusione), 2016/0288 (COD), 12.10.2016, URL: [http://eur-lex.europa.eu/legal-content/IT/ALL/?uri=comnat:COM\\_2016\\_0590\\_FIN](http://eur-lex.europa.eu/legal-content/IT/ALL/?uri=comnat:COM_2016_0590_FIN).

delle sanzioni pecuniarie dovrebbe essere commisurato a questo contesto sensibile. Proprio tale contesto costituisce anche il motivo per cui è importante attuare l'armonizzazione in tutta l'UE, al fine di garantire lo stesso livello elevato di protezione nell'intero territorio interessato. L'articolo 23 del proposto regolamento prevede sanzioni efficaci in caso di violazioni del regolamento, simili al livello di sanzioni pecuniarie inflitte per la violazione delle norme del regolamento generale sulla protezione dei dati, fatta eccezione per taluni aspetti (cfr. osservazioni al punto 38).

7. Anche l'**eliminazione** da tale legislazione **di norme specifiche di notifica di violazioni dei dati** va accolta con favore al fine di evitare sovrapposizioni inutili con le prescrizioni in materia di violazioni dei dati sancite dal regolamento generale sulla protezione dei dati.
8. Altrettanto **positivo è il fatto che l'attenzione sia ora posta sull'erogazione di un pari livello di protezione a tutti gli utenti finali**, in quanto il proposto regolamento ha dispensato dalla nozione di differenziamiento tra "abbonati" e altri utenti di servizi di comunicazione elettronica.

*ESTENSIONE DELL'AMBITO DI APPLICAZIONE RISPETTO ALLA DIRETTIVA RELATIVA ALLA VITA PRIVATA E ALLE COMUNICAZIONI ELETTRONICHE*

9. Il Gruppo di lavoro accoglie con favore l'**espansione dell'ambito di applicazione del proposto regolamento ai fornitori di servizi over-the-top (OTT)**, ossia servizi che sono equivalenti sotto il profilo funzionale a mezzi di comunicazione più tradizionali e presentano quindi potenzialmente possibilità analoghe di avere ripercussioni sulla vita privata e sul diritto alla segretezza delle comunicazioni dei cittadini dell'UE. Il Gruppo di lavoro accoglie con particolare favore il fatto che tutte le categorie OTT (OTT0, OTT1 e talune OTT2)<sup>6</sup> rientrino nell'ambito di applicazione del regolamento in quanto esso non riguarda soltanto i mezzi di comunicazione tradizionali (OTT0), ma anche i servizi equivalenti sotto il profilo funzionale (OTT1) di cui all'articolo 8, paragrafo 1, lettera c) del proposto regolamento. Inoltre, è positivo che, oltre alle definizioni ai sensi del codice europeo delle comunicazioni elettroniche, alcuni servizi OTT2 siano inclusi laddove forniscano una comunicazione interpersonale e interattiva accessoria intrinsecamente connessa ad altri servizi dei fornitori degli stessi, come ad esempio nel caso di giochi, applicazioni per incontri o siti di recensioni (articolo 4, paragrafo 2, del proposto regolamento). Analogamente, altrettanto positivo è **il chiarimento secondo il quale la protezione riguarda anche l'interazione da macchina a macchina**. Il considerando 12 chiarisce che i dispositivi che comunicano tra di loro rientrano nell'ambito di applicazione della protezione

---

<sup>6</sup> Per un'ulteriore spiegazione di questi termini cfr. BEREC, *Report on OTT Services* (in inglese) [Relazione sui servizi OTT], BoR (16) 35, 29 gennaio 2016, pag. 15 e 16, URL: [http://berec.europa.eu/eng/document\\_register/subject\\_matter/berec/reports/5751-berec-report-on-ott-services](http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services). Si noti altresì il commento contenuto nella relazione secondo il quale le categorie sono intese come concetti da utilizzare nel dibattito sulla revisione e non sono intesi costituire concetti giuridici.



previsto dal proposto regolamento. Ciò è auspicabile, in quanto tali comunicazioni contengono spesso informazioni protette dai diritti alla tutela della vita privata. Tuttavia, l'applicabilità di tale protezione potrebbe essere chiarita (cfr. osservazione al punto 40, lettera h)).

10. Il Gruppo ritiene che sia positivo anche il fatto che **il proposto regolamento tratti in maniera chiara i contenuti e i metadati associati**. Il considerando 14 chiarisce che la definizione di cui all'articolo 4, paragrafo 3, lettera a), di "dati delle comunicazioni elettroniche" va intesa in maniera sufficientemente ampia da coprire *tutti* i contenuti e tutti i metadati associati, indipendentemente, ad esempio, dai mezzi di trasmissione di segnali. Tuttavia, il Gruppo di lavoro osserva come aspetto che desta preoccupazione nell'osservazione di cui al punto 39 che questa attuale definizione di "dati delle comunicazioni elettroniche" è ancora oggetto di discussione. In linea con tale espansione dell'ambito di applicazione, il Gruppo di lavoro rileva che **il riconoscimento del fatto che i metadati possono rivelare dati estremamente sensibili** (cfr. il punto 2.2 della relazione; considerando 2) costituisce un'aggiunta essenziale. Il Gruppo di lavoro accoglie con favore il fatto che la Commissione europea, così facendo, incorpori le considerazioni espresse dalla Corte in relazione alle cause *Digital Rights Ireland* e *Tele2/Watson*. Il Gruppo apprezza altresì il **riconoscimento del fatto che l'analisi dei contenuti costituisca un trattamento a rischio elevato**. Il considerando 19 e l'articolo 6, paragrafo 3, lettera b), stabiliscono la presunzione giuridica logica secondo la quale la scansione del contenuto sia un trattamento a rischio elevato a norma dell'articolo 35 del regolamento generale sulla protezione dei dati e, a prescindere dall'esistenza di un rischio residuo elevato, richiede sempre una consultazione preventiva dell'autorità (capofila) di protezione dei dati. Allo stesso tempo, il Gruppo di lavoro esprime preoccupazioni in merito all'ambito di applicazione della definizione di "metadati" e al fatto che l'analisi dei metadati non è soggetta al medesimo requisito obbligatorio di svolgimento di una valutazione d'impatto sulla protezione dei dati (cfr. osservazioni ai punti 33 e 46).
11. Il continuo **riconoscimento dell'importanza dell'anonimizzazione** è anch'esso accolto con favore. Nella direttiva relativa alla vita privata e alle comunicazioni elettroniche, le misure di anonimizzazione sono già state importanti per assicurare la compatibilità (ad esempio l'articolo 6, paragrafo 1, di detta direttiva afferma che i dati sul traffico devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione di una comunicazione). L'articolo 6, paragrafo 2, lettera c) e l'articolo 6, paragrafo 3, lettera b), del proposto regolamento, consentono un'eccezione al divieto di trattamento di metadati e contenuti a fronte dell'ottenimento del consenso relativo, purché il o i fini in questione "non possano essere realizzati mediante un trattamento anonimizzato delle informazioni". Richiedere tali misure di tutela della vita privata oltre a chiedere il consenso degli utenti protegge questi ultimi da trattamenti ingiustificati. Tuttavia, allo stesso tempo, il Gruppo di lavoro nutre una grave preoccupazione in merito al fatto che l'adozione di tali tecniche di anonimizzazione non sarebbe necessaria per il tracciamento dell'ubicazione degli utenti attraverso le loro apparecchiature mobili (cfr. osservazioni al punto 17). Inoltre, anche qualora si debbano applicare misure di anonimizzazione, i fornitori dovrebbero sempre svolgere una valutazione d'impatto sulla protezione dei dati (cfr. osservazioni ai punti 33 e 46) e il Gruppo di lavoro chiede che venga imposto l'obbligo

supplementare di rendere pubbliche le modalità di anonimizzazione e aggregazione dei dati (cfr. osservazioni al punto 42, lettera b)).

12. Un altro aspetto positivo è l'**ampia formulazione della protezione delle apparecchiature terminali**. Il considerando 20 e l'articolo 8 stabiliscono che le tecnologie utilizzate per accedere alle apparecchiature terminali non sono rilevanti: qualsiasi interferenza con l'apparecchiatura terminale, incluso l'utilizzo delle sue capacità di elaborazione, richiede il consenso dell'utente finale (con talune eccezioni). La Commissione europea ha ora confermato con fermezza che la rilevazione delle "impronte digitali per accedere al dispositivo" rientra nell'ambito di applicazione di questa disposizione. Inoltre, il Gruppo di lavoro accoglie con favore il fatto che sia stato sottolineato che le preferenze espresse da una persona nelle **impostazioni relative alla vita privata di un navigatore siano applicabili** e vincolanti nei confronti di terzi come descritto al considerando 22. Ciò è utile nelle situazioni in cui un terzo (ad esempio una rete di annunci pubblicitari) non rispetti tali impostazioni. Tuttavia, questo aspetto dovrebbe anche essere stabilito in una disposizione pertinente del proposto regolamento.
13. Infine, è positiva anche la continua **inclusione delle persone giuridiche nell'ambito di applicazione del proposto regolamento** (cfr. relazione, punto 2.2; considerando 3, 33 e 42; articolo 1, articolo 15 e articolo 16, paragrafo 5). Ciò è già stato attuato nel contesto della direttiva relativa alla vita privata e alle comunicazioni elettroniche, tuttavia, dato che le autorità di protezione dei dati saranno incaricate di fare rispettare le nuove norme, è utile sottolinearlo in modo specifico. Ciò consente alle autorità di protezione dei dati di intervenire nei casi in cui le persone giuridiche siano vittime di un'infrazione, ad esempio quando le imprese ricevono *spam* o le loro comunicazioni vengono monitorate surrettiziamente. Tuttavia, il gruppo di lavoro osserva altresì, come aspetti di preoccupazione, che l'applicazione del consenso alle persone giuridiche non è chiara (cfr. osservazione al punto 41, lettera a)) e non è chiaro che cosa si intenda per "interesse legittimo" di persone giuridiche nel caso della commercializzazione diretta (cfr. osservazione al punto 43, lettera c)).

14. Il gruppo di lavoro accoglie con favore un'altra categoria di miglioramenti legati all'applicazione e all'interpretazione del concetto di consenso. Innanzitutto, è positivo **il chiarimento che l'accesso a Internet e la telefonia (mobile) sono servizi essenziali e i fornitori di questi servizi non possono "forzare" i propri clienti ad acconsentire ad alcun trattamento di dati non necessario per la fornitura del servizio essenziale stesso**. Nel considerando 18 si rileva, in particolare, che i servizi di accesso a internet a banda larga e di comunicazione vocale vanno considerati servizi essenziali, il che significa che, data la dipendenza delle persone dall'accesso a tali servizi, il consenso per il trattamento dei loro dati delle comunicazioni per finalità aggiuntive (ad esempio trattamento per finalità pubblicitarie o di commercializzazione) non può essere valido. Al contempo, il Gruppo di lavoro nutre la preoccupazione che questo chiarimento sia troppo limitato. Anche i servizi offerti da taluni fornitori di servizi *over-the-top* possono essere considerati come servizi essenziali e il regolamento sulla vita privata e le comunicazioni elettroniche dovrebbe altresì proibire specificamente scelte del tipo "prendere o lasciare" in altre circostanze (cfr. osservazione al punto 20).
15. Inoltre, è positiva **l'armonizzazione dell'obbligo di ottenere il consenso per l'inclusione di dati personali di persone fisiche in elenchi**. A norma dell'articolo 15 del proposto regolamento, il trattamento di dati nel contesto di elenchi pubblici è consentito soltanto con il consenso delle persone fisiche e laddove alle persone giuridiche sia data la possibilità di contestare. Questo aspetto è trattato ulteriormente al considerando 31 dove si sottolinea che tale consenso deve essere specifico per quanto riguarda le categorie particolari di dati personali da includere nell'elenco. Tuttavia, il Gruppo di lavoro osserva, come sua preoccupazione, che il proposto regolamento potrebbe essere più chiaro e specificare che per eventuali attività di ricerca e ricerca inversa sarà necessario un consenso separato specifico (cfr. osservazione al punto 37).
16. Apprezzata è anche **la nuova eccezione mirata per le interferenze non intrusive con le apparecchiature terminali**. Il Gruppo di lavoro ritiene utile che il proposto regolamento chiarisca che il divieto non si applica alla misurazione del traffico in un sito (nel rispetto dell'eccezione di limitata portata che prevede che tale misurazione sia effettuata dal fornitore del servizio della società dell'informazione richiesto dall'utente finale, cfr. articolo 8, paragrafo 1, lettera d), del proposto regolamento). Cfr. anche il considerando 21. In ogni caso, il Gruppo di lavoro suggerisce di utilizzare una definizione più neutra della tecnologia e di chiarire l'applicabilità di tale eccezione (cfr. osservazione al punto 25).

### 3. ASPETTI DI GRAVE PREOCCUPAZIONE

#### *LA TUTELA GARANTITA DAL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI VIENE COMPROMESSA DAL REGOLAMENTO PROPOSTO*

Come già accennato, il regolamento proposto contiene vari miglioramenti fondamentali; tuttavia, presenta anche aspetti che destano preoccupazione, secondo livelli di gravità

diversi. In questa sezione il Gruppo di lavoro esamina i quattro aspetti per i quali nutre **gravi preoccupazioni**. Si tratta nello specifico di disposizioni che **compromettono il livello di protezione garantito dal regolamento generale sulla protezione dei dati**.

17. **Gli obblighi previsti dal regolamento per il tracciamento dell'ubicazione delle apparecchiature terminali dovrebbero essere conformi ai requisiti del regolamento generale sulla protezione dei dati.** L'articolo 8, paragrafo 2, lettera b), del proposto regolamento impone, ai fini dell'ammissibilità della raccolta di informazioni emesse dall'apparecchiatura terminale, soltanto la visualizzazione di un avviso e l'attuazione di misure di sicurezza. Precisa inoltre che il responsabile della raccolta deve indicare ogni misura a disposizione dell'utente finale dell'apparecchiatura terminale per arrestare o minimizzare tale raccolta. Così facendo, l'articolo 8, paragrafo 2, lettera b), dà l'impressione che le organizzazioni possano raccogliere informazioni emesse dalle apparecchiature terminali per tenere traccia degli spostamenti fisici delle persone (ad esempio "tracciamento WiFi" o "tracciamento Bluetooth") senza il consenso dell'interessato. La parte che raccoglie questi dati potrebbe apparentemente conformarsi alla norma tramite un avviso che informa gli utenti di spegnere i loro dispositivi quando non desiderano essere tracciati. Tale approccio è contrario all'obiettivo fondamentale della politica della Commissione europea in materia di telecomunicazioni di fornire connettività Internet mobile ad alta velocità, con una forte protezione della vita privata, a basso costo, a tutti gli europei, anche a livello transfrontaliero.

Inoltre, il proposto regolamento non impone alcuna chiara limitazione in merito alla finalità della raccolta dei dati o delle successive attività di trattamento. In questo contesto, va osservato che tali indirizzi MAC sono dati personali e lo restano anche dopo l'adozione di misure di sicurezza quali l'*hashing*. Non sussistendo ulteriori obblighi o limitazioni, il livello di protezione di tali dati personali nel quadro del proposto regolamento è notevolmente inferiore rispetto a quello previsto dal regolamento generale sulla protezione dei dati, secondo il quale tale tracciamento dovrebbe essere corretto, lecito e trasparente. Il considerando 25 rileva inoltre inutilmente che alcune delle funzionalità di tracciamento WiFi non comportano rischi elevati per la vita privata, mentre altre possono essere lesive, come per esempio quelle che tracciano le persone nel tempo. Sebbene il Gruppo di lavoro apprezzi il riconoscimento che quest'ultima funzionalità ponga rischi elevati per la vita privata, non è utile stabilire a priori che talune altre funzionalità non sono lesive, senza ulteriori valutazioni delle circostanze e della proporzionalità del trattamento. Tale valutazione dovrebbe essere effettuata tenendo conto delle seguenti condizioni relative al tracciamento WiFi non anonimizzato.

A seconda delle circostanze e delle finalità della raccolta dei dati, a norma del regolamento generale sulla protezione dei dati è probabile che tale tracciamento sia soggetto al consenso o possa essere effettuato soltanto se i dati personali raccolti vengono anonimizzati. È preferibile che tale anonimizzazione venga effettuata immediatamente dopo la raccolta. Qualora l'anonimizzazione immediata non sia possibile in considerazione delle finalità per le quali vengono raccolti i dati, questi ultimi possono essere trattati durante un arco di tempo nel quale non sono anonimizzati soltanto qualora siano soddisfatte le seguenti condizioni: i) la finalità della raccolta dei dati deve essere limitata a un mero conteggio statistico (cfr. esempi riportati in appresso); ii) il tracciamento è limitato nel tempo e nello spazio nella misura strettamente necessaria a tale finalità; iii) i dati vengono cancellati o anonimizzati immediatamente dopo; e iv) deve essere offerta un'effettiva possibilità

di esclusione (*opt-out*). In tutti i casi, i titolari del trattamento devono ovviamente rispettare l'obbligo di fornire informazioni adeguate.

Il Gruppo di lavoro è preoccupato per il fatto che la potenziale offerta di un singolo *opt-out* per ciascuna organizzazione che raccoglie questi dati costituirebbe un onere inaccettabile per i cittadini, in considerazione dell'aumento dell'utilizzo di tali tecnologie di tracciamento da parte di organizzazioni tanto del settore privato quanto di quello pubblico. Di conseguenza, il Gruppo di lavoro invita il legislatore europeo a promuovere lo sviluppo di norme tecniche che consentano ai dispositivi di segnalare automaticamente un'obiezione contro tale tracciamento e garantiscano al contempo l'esecutività dell'adesione a tale segnale.

Ad esempio, a norma del regolamento generale sulla protezione dei dati sarebbe probabilmente necessario ottenere il consenso degli interessati qualora un titolare del trattamento raccolga e conservi indirizzi MAC indirettamente identificabili (WiFi o Bluetooth) dei dispositivi e calcoli l'ubicazione dell'utente, al fine di tenere traccia della sua posizione nel corso del tempo, ad esempio, nel contesto di più negozi. Ciò si verifica in particolare quanto tale tracciamento avviene nel contesto di spazi pubblici, dove gli utenti fanno affidamento legittimamente sul fatto di non essere identificati o tracciati e invece si raccolgono gli indirizzi MAC dei passanti. Tale consenso può essere ottenuto ad esempio con l'aiuto di un'applicazione che invita gli utenti ad acconsentire al tracciamento della loro ubicazione in aree specifiche in cambio di offerte commerciali oppure mettendo a disposizione punti di accettazione all'interno di ubicazioni specifiche oppure tramite un modulo di consenso nell'ambito degli hotspot WiFi.

I titolari del trattamento potrebbero essere autorizzati a trattare le informazioni emesse dalle apparecchiature terminali con la finalità di tracciarne gli spostamenti fisici senza il consenso dell'interessato soltanto in un numero ristretto di circostanze.

Ad esempio, ciò potrebbe verificarsi qualora la finalità sia il conteggio del numero di clienti presenti all'interno di una determinata ubicazione oppure quando si raccolgono i dati emessi su entrambi i lati di un punto di controllo di sicurezza per visualizzare il tempo di attesa. Tuttavia, in entrambi gli esempi i dati dovrebbero essere cancellati o anonimizzati non appena viene soddisfatta la finalità statistica. Ciò significa che gli indirizzi MAC dei dispositivi dei visitatori all'interno di una determinata ubicazione, come ad esempio un negozio, devono essere anonimizzati immediatamente dopo la raccolta, senza alcuna conservazione permanente di tali indirizzi e in maniera tale da escludere dal punto di vista tecnico una reidentificazione degli stessi. Nel caso del calcolo del tempo di attesa, gli indirizzi MAC dovrebbero essere cancellati o anonimizzati non appena i dati non sono più pertinenti per calcolare il tempo di attesa (ad esempio perché il visitatore è giunto all'altro lato del controllo di sicurezza o perché ha lasciato la coda).

Inoltre, il titolare del trattamento dei dati dovrebbe rispettare i requisiti relativi alla minimizzazione dei dati (ad esempio, non effettuando un tracciamento per 24 ore al giorno, 7 giorni su 7, quando la finalità è limitata agli orari di apertura del negozio e/o ricorrendo al campionamento a intervalli). I titolari del trattamento devono altresì adottare altre misure di attenuazione al fine di assicurare che gli impatti sui diritti alla tutela della vita privata degli utenti siano assenti o notevolmente limitati, ad esempio

al fine di proteggere la vita privata delle persone che vivono nei pressi di un punto di raccolta di tali dati.

La scelta espressa dall'articolo 8, paragrafo 2, del proposto regolamento di imporre un semplice obbligo di avviso è ancor più rimarchevole se si considera la conclusione di cui al considerando 20 secondo la quale le informazioni relative al dispositivo dell'utente finale possono anche essere raccolte in remoto a fini di identificazione e tracciabilità e tali trattamenti, sempre secondo il proposto regolamento, possono seriamente compromettere la vita privata di tali utenti finali. Inoltre, l'obbligo non va oltre l'obbligo di informazione già previsto dagli articoli 13 e 14 del regolamento generale sulla protezione dei dati. La grave intrusione nella vita privata causata dal tracciamento è ulteriormente aggravata dall'accesso potenziale di altri ai dati raccolti, si pensi ad esempio alla possibilità che le forze dell'ordine identifichino gli utenti finali sulla base degli indirizzi MAC trasmessi dai loro dispositivi mobili.

**18. Occorre elaborare le condizioni nelle quali è consentita l'analisi dei contenuti e dei metadati.**

L'articolo 6 del proposto regolamento garantisce livelli diversi di protezione per i metadati e i contenuti. Il Gruppo di lavoro non sostiene tale differenziazione: entrambe le categorie di dati sono altamente sensibili. Di conseguenza, i metadati e i contenuti dovrebbero beneficiare degli stessi livelli elevati di protezione. Il punto di partenza dovrebbe quindi essere che è proibito trattare metadati e contenuti senza il consenso di tutti gli utenti finali (ad esempio, del mittente e del destinatario).

A seconda delle finalità, tuttavia, taluni trattamenti potrebbero essere ammessi in assenza di consenso laddove siano strettamente necessari per tali finalità:

- i fornitori possono trattare i dati delle comunicazioni elettroniche per le finalità di cui all'articolo 6, paragrafo 1, lettere a) e b), all'articolo 6, paragrafo 2, lettere a) e b), del proposto regolamento<sup>7</sup>;
- sarebbe opportuno chiarire che talune tecniche di rilevamento/filtraggio dello *spam* e di mitigazione del fenomeno delle reti zombie (*botnet*) possono anche essere considerate strettamente necessarie per il rilevamento o l'arresto dell'uso abusivo dei servizi di comunicazione elettronica (articolo 6, paragrafo 2, lettera b)). Per quanto concerne il filtraggio dello *spam*, agli utenti finali che ricevono *spam* dovrebbero essere offerte, laddove tecnicamente possibile, scelte di esclusione (*opt-out*) granulari;
- sarebbe opportuno chiarire che l'analisi dei dati delle comunicazioni elettroniche per finalità di servizio al cliente può anche rientrare nell'eccezione relativa al trattamento "necessario a fini di fatturazione" (cfr.

---

<sup>7</sup> Per quanto concerne la necessità di soddisfare requisiti di qualità obbligatori, come indicato all'articolo 6, paragrafo 2, lettera a), del proposto regolamento, i fornitori dovrebbero tener conto delle condizioni descritte nel regolamento (UE) 15/2120 (EECS) in particolare l'articolo 3 e i considerando 10 e 13-15. In conformità con tale disposizione, potrebbe essere richiesto ai fornitori di trattare i dati delle comunicazioni per rilevare e filtrare *malware* e *spyware* e gli stessi possono essere autorizzati a comprimere i dati.

articolo 6, paragrafo 2, lettera b)). I metadati pertinenti possono essere conservati fino allo scadere del termine entro il quale è possibile a norma di legge contestare una fattura o sollecitare un pagamento ai sensi del diritto interno. I dati pertinenti (ad esempio gli URL) possono essere conservati soltanto su richiesta dell'utente finale e, in tal caso, soltanto fino alla fine del periodo nel quale una fattura può essere legalmente contestata o un pagamento può essere preteso, conformemente al diritto nazionale (il che significa che l'articolo 7, paragrafo 3, dovrebbe essere modificato);

- si dovrebbe consentire il trattamento di dati delle comunicazioni elettroniche per finalità di erogazione di servizi esplicitamente richiesti da un utente finale, come ad esempio nel caso di una funzionalità di ricerca o indicizzazione di parole chiave, assistenti virtuali, motori di conversione da testo a voce e servizi di traduzione. Ciò richiede l'introduzione di un'esenzione per l'analisi di tali dati per un uso puramente individuale (domestico), nonché per un uso individuale correlato al lavoro<sup>8</sup>. Ciò sarebbe quindi possibile senza il consenso di tutti gli utenti finali, ma potrebbe avvenire solo con il consenso dell'utente finale che richiede il servizio. Tale consenso specifico precluderebbe altresì al fornitore la possibilità di utilizzare tali dati per finalità diverse.

Ciò significa che l'analisi di contenuti e/o dei metadati per tutte le altre finalità, come ad esempio quelle di analisi, profilazione, pubblicità comportamentale o altre finalità a vantaggio (commerciale) del fornitore, richiede l'ottenimento del consenso da parte di tutti gli utenti finali i cui dati verrebbero trattati. In merito a tali situazioni, il proposto regolamento dovrebbe spiegare che il mero atto di inviare un messaggio di posta elettronica o un altro tipo di comunicazione personale da un altro servizio a un utente finale che ha personalmente acconsentito al trattamento dei suoi contenuti e metadati (ad esempio nel corso della sottoscrizione del servizio di posta elettronica), non costituisce un consenso valido per il mittente.

Infine, sarebbe opportuno chiarire che il trattamento di dati di persone diverse dagli utenti finali (ad esempio l'immagine o la descrizione di una terza persona in uno scambio tra due persone) comporta altresì la necessità di rispettare tutte le pertinenti disposizioni del regolamento generale sulla protezione dei dati.

- 19. Le apparecchiature terminali e i programmi devono *per impostazione predefinita* scoraggiare, prevenire e vietare interferenze illecite con gli stessi e fornire informazioni sulle opzioni.** Sebbene il proposto regolamento obblighi i fornitori di programmi a consentire alle comunicazioni elettroniche di "offrire l'opzione" di prevenire una forma limitata di interferenza con le apparecchiature terminali e, all'atto dell'installazione, obblighi i fornitori di programmi a chiedere all'utente finale di

---

<sup>8</sup> Sebbene il considerando 13 del proposto regolamento escluda esplicitamente le reti aziendali dall'ambito di applicazione del regolamento, questa nuova eccezione per l'uso individuale dovrebbe riguardare anche l'utilizzo di servizi *cloud* da parte di dipendenti per l'uso correlato al lavoro, come ad esempio lo svolgimento di ricerche nelle loro caselle di posta elettronica.



acconsentire a una data impostazione (articolo 10, paragrafi 1 e 2), tale scelta non è sinonimo di *tutela della vita privata per impostazione predefinita*. Inoltre, attualmente esiste già una "opzione" per prevenire talune interferenze e finora ciò non ha portato a risultati sufficienti nella gestione del problema del tracciamento ingiustificato. Ed è esattamente per questo motivo che nel regolamento generale sulla protezione dei dati è stata operata la scelta politica consapevole di introdurre i principi della protezione dei dati e della vita privata fin dalla progettazione e protezione per impostazione predefinita (articolo 25 del regolamento generale sulla protezione dei dati). Il proposto regolamento compromette tali principi in relazione ai dati delle comunicazioni e dei dispositivi. Nel frattempo, la direttiva 2014/53/UE<sup>9</sup> sulle apparecchiature radio (menzionata al considerando 10) prevede un obbligo di sicurezza molto limitato che impone alle apparecchiature radio di contenere "elementi di salvaguardia per garantire la protezione dei dati personali e della vita privata dell'utente e dell'abbonato" (articolo 3, paragrafo 3, lettera e)). Ciò non può sostituire impostazioni specifiche di tutela della vita privata per impostazione predefinita nel quadro del proposto regolamento. A tale proposito è altresì opportuno osservare che l'indagine Eurobarometro, pubblicata nel dicembre 2016 (in inglese), in materia di e-Privacy osserva che "pressoché sette persone su dieci (69 %) sono pienamente d'accordo in merito al fatto che le impostazioni predefinite del loro navigatore dovrebbero impedire la condivisione di informazioni"<sup>10</sup>. Il Gruppo di lavoro nutre una preoccupazione distinta per quanto riguarda le impostazioni del navigatore e la definizione di "terzi". Cfr. osservazione al punto 24. Inoltre, andrebbe tenuto presente che questa disposizione non riguarda soltanto i navigatori utilizzati sui computer, ma si estende anche ad altri tipi di programmi che consentono la comunicazione (ivi inclusi sistemi operativi, applicazioni e interfacce software per dispositivi collegati a Internet delle cose). In sintesi, le apparecchiature terminali e i programmi devono *per impostazione predefinita* offrire impostazioni che proteggano la vita privata e guidare gli utenti attraverso i menu di configurazione in caso di scostamento da queste impostazioni predefinite al momento dell'installazione. Tali menu di configurazione dovrebbero sempre essere facilmente accessibili durante l'uso. Il Gruppo di lavoro incoraggia il legislatore europeo a chiarire l'ambito di applicazione dell'articolo 10 a tal fine.

- 20. Il regolamento sulla vita privata e le comunicazioni elettroniche dovrebbe vietare esplicitamente il ricorso a barriere di tracciamento (*tracking wall*),** ossia la pratica tramite la quale l'accesso a un sito web o a un servizio viene negato a meno che le persone non acconsentano a essere tracciate su altri siti web o servizi. Come già osservato in precedenti pareri del Gruppo di lavoro sulla direttiva relativa alla vita privata e alle comunicazioni elettroniche<sup>11</sup>, tali approcci di tipo "prendere o lasciare" sono raramente legittimi<sup>12</sup>. Quando l'utilizzo delle capacità di trattamento e

---

<sup>9</sup> Direttiva 2014/53/UE sulle apparecchiature radio.

<sup>10</sup> Cfr. *Flash Eurobarometer 443*, Relazione sulla e-Privacy (in inglese) (pubblicato nel dicembre 2016), pag. 5.

<sup>11</sup> Cfr. ad esempio WP 240 (riesame della direttiva relativa alla vita privata e alle comunicazioni elettroniche), pag. 16; WP 208 (esenzione dal consenso), pag. 5.

<sup>12</sup> Tale posizione non pregiudica l'articolo 7, paragrafo 4, del regolamento generale sulla protezione dei dati, che può anch'esso precludere opzioni del tipo "prendere o lasciare" in altre situazioni laddove ciò sia opportuno.

conservazione dell'apparecchiatura terminale o la raccolta di informazioni provenienti dalle apparecchiature terminali degli utenti finali consentono il tracciamento delle attività dell'utente nel corso del tempo o nell'ambito di diversi servizi (ad esempio siti web o applicazioni diversi), tali trattamenti possono compromettere seriamente la vita privata di tali utenti. Data l'importanza fondamentale di Internet nel consentire l'esercizio del diritto fondamentale di libertà di espressione, ivi incluso il diritto di accesso alle informazioni, la capacità delle singole persone di accedere a contenuti online non dovrebbe dipendere dall'accettazione delle attività di tracciamento su tutti i dispositivi e i siti web/le applicazioni. Di conseguenza il futuro regolamento sulla vita privata e le comunicazioni elettroniche dovrebbe specificare che l'accesso a contenuti presenti, ad esempio, su siti web e in applicazioni, non può essere subordinato all'accettazione di tali attività intrusive di trattamento, indipendentemente dalla tecnologia di tracciamento applicata, come ad esempio marcatori, impronte digitali per accedere al dispositivo, inoculazione di identificativi unici o altre tecniche di monitoraggio. La necessità di tale divieto è sottolineata dalla recente indagine Eurobarometro sull'e-Privacy che sottolinea che "circa due terzi dei partecipanti afferma che sia inaccettabile che le loro attività online siano monitorate in cambio di un accesso illimitato a un determinato sito web (64 %)".

21. In sintesi, per quanto riguarda i quattro aspetti menzionati in precedenza, **il proposto regolamento dovrebbe mantenere la promessa di fornire un livello di protezione analogo o superiore a quello garantito dal regolamento generale sulla protezione dei dati**. Il considerando 5 rileva che il regolamento proposto non riduce il livello di protezione garantito dal regolamento generale sulla protezione dei dati. Tuttavia, allo stato attuale del proposto regolamento, tale affermazione non è corretta, in particolare per quanto riguarda il tracciamento di dispositivi (osservazione al punto 17), l'assenza del principio della tutela della vita privata per impostazione predefinita (osservazione al punto 19) e il consenso (osservazione al punto 18). Ciò è particolarmente rilevante, in quanto nel medesimo considerando si afferma che il proposto regolamento sarà una "*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". Il Gruppo di lavoro suggerisce che, quanto meno, il testo del regolamento sulla vita privata e le comunicazioni elettroniche chiarisca che:

- i) i divieti sanciti dal regolamento sulla vita privata e le comunicazioni elettroniche hanno priorità rispetto ai permessi concessi dal regolamento generale sulla protezione dei dati (ad esempio, il divieto di interferenza a norma dell'articolo 5 del regolamento sulla vita privata e le comunicazioni elettroniche ha la precedenza sui diritti dei fornitori di servizi di comunicazione elettronica di trattare ulteriormente i dati personali a norma dell'articolo 5, paragrafo 1, lettera b), e dell'articolo 6, paragrafo 4, del regolamento generale sulla protezione dei dati);
- ii) laddove il trattamento sia consentito ai sensi di qualsiasi eccezione (ivi incluso in relazione al consenso) ai divieti sanciti dal regolamento sulla vita privata e le comunicazioni elettroniche, tale trattamento, qualora riguardi dati personali, deve comunque rispettare tutte le disposizioni pertinenti del regolamento generale sulla protezione dei dati;
- iii) quando il trattamento è consentito ai sensi di qualsiasi eccezione ai divieti sanciti dal regolamento sulla vita privata e le comunicazioni elettroniche,

qualsiasi altro trattamento a norma del regolamento generale sulla protezione dei dati deve essere proibito, ivi incluso il trattamento per altre finalità sulla base dell'articolo 6, paragrafo 4, del regolamento generale sulla protezione dei dati. Ciò non impedirebbe ai titolari del trattamento di chiedere un consenso aggiuntivo per nuovi trattamenti, né impedirebbe ai legislatori di definire ulteriori eccezioni limitate e specifiche nel regolamento sulla vita privata e le comunicazioni elettroniche, ad esempio, per consentire il trattamento per finalità scientifiche o statistiche ai sensi dell'articolo 89 del regolamento generale sulla protezione dei dati o per proteggere gli "interessi vitali" delle persone ai sensi dell'articolo 6, lettera d), di quest'ultimo regolamento.

Inoltre, il regolamento sulla vita privata e le comunicazioni elettroniche dovrebbe essere interpretato in modo da assicurare che garantisca quanto meno il medesimo livello e, ove appropriato, un livello più elevato di protezione rispetto a quello concesso a norma del regolamento generale sulla protezione dei dati.

#### 4. ALTRI ASPETTI CHE DESTANO PREOCCUPAZIONE

Oltre agli aspetti di cui sopra, il Gruppo di lavoro Articolo 29 **esprime preoccupazione** in merito a quanto segue.

##### *OCCORRE AMPLIARE L'AMBITO DI APPLICAZIONE TERRITORIALE E MATERIALE*

22. **Il termine "metadati" è definito in termini troppo ristretti.** Attualmente questo termine è definito all'articolo 4, lettera c) come "dati trattati in una rete di comunicazione elettronica per trasmettere, distribuire o scambiare il contenuto delle comunicazioni elettroniche" (sottolineatura aggiunta). L'uso della parola "rete" sembra suggerire che solo i dati generati nel contesto dell'erogazione di servizi al livello "inferiore" della rete si qualificerebbero come "metadati". Ciò potrebbe significare che i dati generati nel contesto della fornitura di un servizio OTT sarebbero esclusi da questo ambito di applicazione. Ciò non sarebbe auspicabile e, probabilmente, nemmeno previsto, data l'intenzione di estendere l'ambito di applicazione del proposto regolamento ai fornitori di servizi OTT. Al fine di risolvere questa questione, la definizione di "metadati delle comunicazioni elettroniche" dovrebbe essere modificata in maniera da includere tutti i dati trattati per trasmettere, distribuire o scambiare il contenuto delle comunicazioni elettroniche.

23. Inoltre, una questione che desta preoccupazioni è il fatto che **l'ambito di applicazione del proposto regolamento in relazione alle organizzazioni senza uno stabilimento nell'UE fa riferimento esclusivamente ai fornitori di servizi di comunicazione elettronica.** Ai sensi del proposto regolamento, il fornitore di un servizio di comunicazione elettronica non ubicato nell'UE deve designare per iscritto un rappresentante nell'Unione (articolo 3, paragrafo 2). Al considerando 9 viene menzionato altresì che il regolamento si applica al trattamento da parte di fornitori di servizi di comunicazione elettronica, senza tener conto dell'ubicazione del trattamento. Il Gruppo di lavoro accoglie con favore questo chiarimento. Tuttavia, poiché la formulazione è limitata ai fornitori di servizi di comunicazione elettronica, risulta incerta la misura in cui tale ambito di applicazione si applichi ad altri tipi di

parti (ad esempio alle parti che interferiscono o raccolgono informazioni trasmesse da apparecchiature terminali di utenti finali, cfr. articolo 3, paragrafo 1, lettera c), in combinato disposto con l'articolo 8 del proposto regolamento). Di conseguenza, il Gruppo di lavoro suggerisce la modifica dell'articolo 3, paragrafo 2, e dell'articolo 3, paragrafo 5, al fine di includere i fornitori di elenchi pubblici, i fornitori di programmi che consentono le comunicazioni elettroniche e le persone che inviano comunicazioni commerciali dirette o raccolgono (altre) informazioni relative a o conservate nelle apparecchiature terminali degli utenti finali, qualora le loro attività siano rivolte a utenti ubicati nell'UE (cfr. il considerando 8 del proposto regolamento)<sup>13</sup>.

#### *È NECESSARIO RAFFORZARE LA PROTEZIONE DELLE APPARECCHIATURE TERMINALI*

Un'altra categoria di preoccupazioni è relativa alla protezione insufficiente delle apparecchiature terminali nel contesto del proposto regolamento.

**24. Innanzitutto, il proposto regolamento suggerisce erroneamente che un consenso valido possa essere dato tramite impostazioni non specifiche del navigatore.** Il Gruppo di lavoro prende atto della considerazione che gli utenti finali sono attualmente subissati di richieste di consenso (considerando 22). Le impostazioni del navigatore (e dei programmi comparabili) possono svolgere un ruolo nell'affrontare questo problema, tuttavia, dato che le impostazioni generali del navigatore non sono destinate ad applicarsi all'applicazione di una tecnologia di tracciamento in un caso specifico, non sono idonee per fornire il consenso ai sensi dell'articolo 7 e del considerando 32 del regolamento generale sulla protezione dei dati (in quanto il consenso non è sufficientemente informato e specifico).

L'utente finale deve essere in grado di fornire un consenso distinto per ciascun sito web o ciascuna applicazione in relazione al tracciamento per finalità diverse (ad esempio la condivisione di contenuti sui media sociali o finalità pubblicitarie). Un titolare del trattamento responsabile di numerosi siti web o applicazioni può anche chiedere il consenso per tutti gli altri siti o tutte le altre applicazioni soggetti al suo controllo, a condizione che tale richiesta di consenso sia presentata separatamente.

Inoltre, il titolare del trattamento deve rispettare tutti gli altri obblighi relativi al consenso, ivi incluso quello di fornire agli utenti informazioni adeguate. Per quanto concerne tanto i navigatori quanto i titolari del trattamento dei dati ciò significa che l'offerta della sola opzione di "accettare tutti i marcatori" non sarebbe valida, in quanto ciò non consentirebbe agli utenti di fornire il consenso granulare richiesto. Tuttavia, si dovrebbe fare in modo che i navigatori potessero consentire agli utenti di

---

<sup>13</sup> Cfr. l'articolo 3, paragrafo 2, del regolamento generale sulla protezione dei dati: *"il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione"*. Tale obbligo potrebbe includere anche eccezioni in linea con le disposizioni di cui all'articolo 27, paragrafo 2, del regolamento generale sulla protezione dei dati.

effettuare una scelta informata e consapevole nell'accettare tutti i marcatori, in maniera da prevenire così qualsiasi futura richiesta specifica di consenso proveniente dai siti web che gli utenti visitano.

Il Gruppo di lavoro raccomanda vivamente che il regolamento sulla vita privata e le comunicazioni elettroniche renda obbligatorio per i navigatori attuare meccanismi tecnici quali la norma *Do Not Track* (DNT), al fine di garantire che gli utenti dispongano di una scelta effettiva e del controllo sull'interferenza con i propri dispositivi<sup>14</sup>.

Un aspetto ancora più importante è dato dal fatto che il regolamento sulla vita privata e le comunicazioni elettroniche dovrebbe garantire che tanto la scelta relativa alla conservazione di informazioni nel dispositivo quanto un segnale DNT inviato da un navigatore vengano accettati come indicazione giuridicamente vincolante del consenso o del rifiuto da parte di tutti i titolari del trattamento. Ciò non pregiudica la formulazione di ulteriori orientamenti da parte del Gruppo di lavoro sulla conformità della norma DNT, tra l'altro in relazione al principio della limitazione della finalità, quando detta norma sarà finalizzata (secondo le previsioni verso la fine del 2017).

I tipi impliciti di "consenso" come ad esempio il fare un clic su un sito web o lo scorrimento della pagina, non possono avere priorità rispetto alle scelte relative alla conservazione e al segnale DNT. Un vantaggio importante offerto dall'utilizzo di questa norma è che la stessa non si limita alla tecnologia di tracciamento dei marcatori ma tratta anche altri tipi di tracciamento, come ad esempio l'acquisizione di impronte digitali.

Rendere l'adesione a questa norma giuridicamente obbligatoria risolverà anche un altro problema, ossia quello relativo all'attuale utilizzo del termine "terzi" nell'articolo 10. Solitamente una pagina web o un'applicazione contengono numerosi elementi, appartenenti tanto al sito stesso quanto a siti esterni, e tale codice esterno può anch'esso essere eseguito nel momento in cui si visita un sito web e riportare informazioni a un server appartenente a terzi. Un marcatore di tracciatura può essere inviato da una prima parte quando un utente visita, ad esempio, un sito di social networking. Tale sito di social network potrebbe anche rivestire il ruolo di "terzo" nel momento in cui tale utente visita un altro sito web che contiene un'interazione con il sito di social networking precedentemente visitato. In tutti questi casi, indipendentemente dal fatto che si tratti di "accesso a" o "archiviazione di" informazioni nel dispositivo dell'utente finale, ciò costituisce un'interferenza con il dispositivo, per la quale è richiesto il consenso (a meno che non si applichi una delle eccezioni previste). Nel contesto della norma DNT, tale aspetto viene affrontato utilizzando i termini "a livello di sito" (*site-wide*) e "a livello di Internet" (*Internet-wide*). Di conseguenza, al fine di migliorare la certezza del diritto di tutte le parti interessate, il riferimento a "terzi" contenuto nel regolamento sulla vita privata e le comunicazioni elettroniche dovrebbe essere riformulato in maniera da includere tutte le entità con cui un dispositivo interagisce (in quanto esse archiviano informazioni nel dispositivo o accedono a dette informazioni).

---

<sup>14</sup> Cfr. URL: <https://www.w3.org/TR/tracking-compliance/>. Il paragrafo 7 spiega il modello di eccezione e la distinzione tra le eccezioni a livello di sito e a livello di web. Il paragrafo 6 contiene le informazioni leggibili dalla macchina che i titolari del trattamento possono fornire in termini di requisiti di informazione per ottenere il consenso.

Al fine di rendere la norma *Do Not Track* compatibile con l'elevato livello di protezione della riservatezza delle comunicazioni e della protezione dei dati riconosciuto dalla Carta, il regolamento sulla vita privata e le comunicazioni elettroniche dovrebbe specificare che le richieste di tracciamento a livello di Internet, al contrario del tracciamento a livello di sito, devono essere presentate separatamente e gli utenti devono essere liberi di accettare o negare tali richieste. Inoltre, al fine di proteggere gli utenti dalle frequenti richieste di consenso, il regolamento sulla vita privata e le comunicazioni elettroniche dovrebbe garantire che un rifiuto all'accettazione del tracciamento a livello di Internet da parte di un'organizzazione specifica (tramite la norma *Do Not Track* o tramite una lista nera distinta) impedisca a tale organizzazione di presentare ulteriori future richieste di consenso per almeno 6 mesi. Tale norma non impedisce a detta organizzazione, qualora venga visitata direttamente dall'utente (ossia agisca da "prima parte"), di chiedere il consenso sul proprio sito web (ovvero una richiesta di consenso a livello di sito). In pratica, ciò significa che ad esempio un sito di streaming video che invia marcatori di tracciatura può richiedere il consenso quando tale utente visita il sito di streaming video, ma non può chiedere nuovamente il consenso per un periodo di 6 mesi qualora tale utente abbia rifiutato di acconsentire e visiti altri siti web che contengono video messi a disposizione dal sito web di streaming.

25. Inoltre, **l'eccezione concessa per "misurare il pubblico del web" è formulata in maniera imprecisa.** L'articolo 8, paragrafo 1, lettera d), del proposto regolamento, prevede un'eccezione per la misurazione del pubblico del web. Il primo aspetto che desta preoccupazione è che tale termine è indefinito e può essere confuso con la profilazione degli utenti. La definizione dovrebbe chiarire che tale eccezione non può essere utilizzata per finalità di profilazione. L'eccezione dovrebbe essere applicata soltanto alle analisi di utilizzo necessarie per l'analisi delle prestazioni del servizio richiesto dall'utente, ma non per effettuare analisi relative agli utenti (ovvero analisi del comportamento di utenti identificabili di un sito web, di un'applicazione o di un dispositivo). Di conseguenza, l'eccezione non può essere utilizzata in circostanze nelle quali i dati possono essere collegati a dati di un utente identificabile trattati dal fornitore del servizio o da altri titolari del trattamento. Inoltre, la sua descrizione suggerisce l'applicazione di una tecnologia molto specifica. Di conseguenza il testo "misurare il pubblico del web" dovrebbe essere riformulato in modo neutrale in termini di tecnologia, al fine di includere anche informazioni analoghe usate per finalità analitiche recuperate da applicazioni, dispositivi indossabili e dispositivi di Internet delle cose.

Il Gruppo di lavoro suggerisce di trarre ispirazione dall'eccezione olandese che si applica se strettamente necessario per ottenere informazioni in merito alla qualità tecnica o all'efficacia di un servizio della società dell'informazione fornito e che non ha alcun impatto o ha un impatto minimo sulla vita privata dell'abbonato o dell'utente (finale) interessato (cfr. articolo 11.7a, terzo comma, lettera b) della legge olandese sulle telecomunicazioni). Questa eccezione tiene conto del fatto che la maggior parte dei dati raccolti tramite analisi web o di applicazioni sono comunque dati personali. Ciò significa che il trattamento di questi dati è soggetto anche al regolamento generale sulla protezione dei dati. Pertanto, ciò implica, ad esempio, che l'analisi

dell'utilizzo potrebbe essere eseguita anche da un'organizzazione esterna, ma soltanto se:

- i) tale organizzazione agisce in qualità di responsabile del trattamento;
- ii) è stato stipulato un accordo con il responsabile del trattamento conforme al regolamento generale sulla protezione dei dati;
- iii) la tecnologia di analisi utilizzata impedisce la reidentificazione, ivi incluso, tra l'altro, tramite l'anonimizzazione degli indirizzi IP dagli utenti;
- iv) il marcatore o i marcatori specifici o altri dati utilizzati per l'analisi possono essere utilizzati soltanto per tale specifico sito o dispositivo indossabile o per tale specifica applicazione e non possono essere collegati ad altri dati identificabili;
- v) gli utenti hanno il diritto di opporsi (cfr. osservazioni ai punti 17 e 50 del presente parere).

Anche se il consenso non sarebbe necessario nel caso in cui venissero soddisfatte queste condizioni, i titolari del trattamento devono comunque fornire informazioni adeguate agli utenti, ad esempio, attraverso i campi di rappresentazione dello stato di tracciamento nel quadro della norma *Do Not Track*<sup>15</sup>.

26. Il regolamento sulla vita privata e le comunicazioni elettroniche **dovrebbe garantire eccezioni di limitata portata e formulate con precisione in relazione alle prescrizioni in materia di consenso**. La formulazione dell'eccezione all'obbligo di ottenere il consenso per l'interferenza con i dispositivi di cui all'articolo 8, paragrafo 1, lettera c), è pressoché identica all'attuale formulazione della direttiva relativa alla vita privata e alle comunicazioni elettroniche riportata all'articolo 5, paragrafo 3, *"nella misura strettamente necessaria a fornire un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente"*, tuttavia la parola fondamentale, ossia "strettamente", è stata omessa, senza alcuna spiegazione. Tale aspetto desta preoccupazioni per due motivi. In primo luogo, la disposizione della direttiva relativa alla vita privata e alle comunicazioni elettroniche ha già portato a un'ampia discussione in merito al suo ambito di applicazione tra le autorità di controllo e le organizzazioni e la soppressione della parola "strettamente" fornirà ancora meno certezza giuridica. Inoltre, ciò desta preoccupazioni perché il Gruppo di lavoro ha già fornito orientamenti in merito all'interpretazione del termine "strettamente" in questo contesto. Il Gruppo di lavoro ha suggerito la seguente precisazione nel parere relativo all'esenzione dal consenso per l'uso di *cookie* (WP 194):

*"un cookie deve offrire una funzionalità specifica all'utente (o abbonato): se i cookie sono disabilitati, la funzionalità non sarà disponibile [e] tale funzionalità è stata richiesta esplicitamente dall'utente (o abbonato) nell'ambito di un servizio della società dell'informazione"*.<sup>16</sup>

---

<sup>15</sup> Cfr. *Tracking Preference Expression (DNT)* (in inglese) [Espressione delle preferenze di tracciamento (DNT)], bozza dell'editore, 7 marzo 2016.

<sup>16</sup> Gruppo di lavoro Articolo 29, WP 294, Parere 4/2012 relativo all'esenzione dal consenso per l'uso di cookie, adottato il 7 giugno 2012, URL: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194\\_it.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_it.pdf).

Inoltre, il Gruppo ha chiarito che:

*"i cookie di "terzi" solitamente non sono "strettamente necessar[i]" all'utente che visita il sito web poiché sono in genere connessi a un servizio distinto da quello "esplicitamente richiesto" dall'utente"<sup>17</sup>.*

Il Gruppo di lavoro ha aggiunto che anche l'uso di *plug-in* sociali destinati a non utenti di una piattaforma o di un sito web non sarebbe parimenti da considerare strettamente necessario.

Inoltre, mentre l'articolo 6, paragrafo 1, lettera b) del proposto regolamento consente di trattare i dati delle comunicazioni elettroniche se "necessario" per fini di sicurezza, il considerando 49 del regolamento generale sulla protezione dei dati impone che ciò sia strettamente necessario. L'omissione della parola "strettamente" potrebbe non essere stata intenzionale, in quanto il considerando 21 del proposto regolamento menziona che il consenso per l'interferenza non dovrebbe essere richiesto qualora tale interferenza sia "strettamente" necessaria. Ciò nonostante, il proposto regolamento offre un'opportunità per chiarire ulteriormente che la prova della necessità nel contesto di tale regolamento deve essere interpretata in senso stretto per tutte le eccezioni. Il Gruppo di lavoro suggerisce quindi che, per quanto riguarda tutte le eccezioni di cui all'articolo 6 e all'articolo 8, paragrafo 1, del proposto regolamento, occorre aggiungere la parola "strettamente" davanti a "necessario".

D'altro canto, il regolamento sulla vita privata e le comunicazioni elettroniche dovrebbe consentire esplicitamente l'interferenza con le apparecchiature per installare gli aggiornamenti di sicurezza. Inviare aggiornamenti di sicurezza tramite Internet è il metodo preferito per l'installazione di tali aggiornamenti nella maggior parte dei dispositivi degli utenti finali. L'installazione di aggiornamenti è considerata un'interferenza con l'apparecchiatura terminale. Vi è un interesse legittimo nel garantire che la sicurezza di questi dispositivi rimanga aggiornata. In generale, quindi, un fornitore di *patch* di sicurezza dovrebbe essere in grado di installare gli aggiornamenti di sicurezza strettamente necessari senza il consenso dell'utente finale. Tuttavia non è certo se tale interferenza possa sfruttare l'eccezione al divieto di interferenza relativa alle "società dell'informazione" (articolo 8, paragrafo 1, lettera c)). Sarebbe opportuno chiarire che l'installazione di aggiornamenti di sicurezza è consentita a norma di tale eccezione, tuttavia, soltanto nella misura in cui: i) gli aggiornamenti di sicurezza sono inviati in maniera discreta e non modificano in alcun modo le funzionalità dei programmi sull'apparecchiatura (ivi inclusa l'interazione con altri programmi o con impostazioni scelte dall'utente); ii) l'utente finale viene informato anticipatamente dell'installazione di ciascun aggiornamento; e iii) l'utente finale ha la possibilità di disattivare l'installazione automatica di tali aggiornamenti.

## COMMERCIALIZZAZIONE DIRETTA

---

<sup>17</sup> Ibid.



Un'altra categoria di preoccupazioni riguarda la protezione insufficiente contro la commercializzazione diretta.

27. Innanzitutto, una questione di preoccupazione è il fatto che **l'ambito di applicazione della commercializzazione diretta è troppo limitato**. Nell'articolo 4, paragrafo 3, lettera f), del proposto regolamento, le "comunicazioni di commercializzazione diretta" sono definite come "qualsiasi forma di pubblicità, scritta od orale, inviata a uno o più utenti identificati o identificabili di servizi di comunicazione elettronica". L'uso della parola "inviata" implica l'uso di mezzi tecnologici di comunicazione che comportano necessariamente la trasmissione di una comunicazione, mentre la maggior parte della pubblicità presente sul web (tramite piattaforme di media sociali o su siti web) non comporta "l'invio" di annunci pubblicitari in senso stretto. Ciò è ulteriormente sottolineato dagli esempi riportati in appresso a tale definizione (SMS, posta elettronica) e nel considerando 33. Gli esempi riportati rappresentano forme alquanto tradizionali di comunicazione di commercializzazione e nonostante tutto, l'uso di sistemi di chiamata "alquanto tradizionali" non rientra presumibilmente nell'ambito di applicazione. L'articolo e il considerando devono essere modificati al fine di includere tutta la pubblicità *inviata, indirizzata o presentata* a uno o più utenti finali identificati o identificabili. Inoltre, dovrebbe essere assicurato altresì che anche le pubblicità comportamentali (basate sui profili degli utenti finali) siano considerate comunicazioni di commercializzazione diretta indirizzate a "uno o più utenti finali identificati o identificabili" (in quanto tali pubblicità sono destinate a utenti specifici, identificabili).

Inoltre, in linea con la finalità proposta delle "comunicazioni di commercializzazione diretta", la protezione di cui all'articolo 16, paragrafo 1, sarebbe limitata ai messaggi contenenti materiale pubblicitario e non proteggerebbe le persone da altri messaggi inviati, indirizzati o presentati per fini commerciali (ad esempio messaggi per la generazione di contatti (*lead-generation*) che chiedono il consenso, la promozione di opinioni politiche o preferenze di voto, la promozione di organismi di beneficenza o altre organizzazioni senza scopo di lucro oppure messaggi generali di promozione del marchio di un'organizzazione). Inoltre, i telefax sono ancora in uso come metodo per la commercializzazione diretta, anche se non sono menzionati nella definizione. L'articolo 4, paragrafo 3, lettera f) dovrebbe pertanto includere qualsiasi tipo di pubblicità, propaganda o promozione, anche a favore di organizzazioni senza scopo di lucro, e dovrebbe includere esplicitamente i telefax, nonché la posta elettronica e gli SMS (cfr. anche il suggerimento per il chiarimento riportato nell'osservazione al punto 43 a)). Infine, il considerando 32 afferma che la commercializzazione diretta include i messaggi inviati dai partiti politici per promuovere sé stessi. Tale affermazione dovrebbe essere aggiornata per includere politici e candidati alle elezioni che promuovono la loro candidatura.

28. In secondo luogo, **la revoca del consenso per la commercializzazione diretta non è gratuito e non è così facile da dare come invece nel caso della concessione del consenso**. Occorre chiarire l'opzione di revoca del consenso a norma del proposto regolamento al fine di garantire la coerenza e migliorare la protezione dei destinatari. L'articolo 16, paragrafo 6 del proposto regolamento prevede attualmente che i destinatari della commercializzazione diretta debbano essere informati circa "le

informazioni necessarie affinché possano esercitare agevolmente il loro diritto di revoca del consenso a ricevere ulteriori messaggi commerciali" (sottolineatura aggiunta). Ciò è confermato al considerando 34. Dal considerando 70 del regolamento generale sulla protezione dei dati si desume tuttavia che gli interessati a norma del regolamento generale sulla protezione dei dati non dovrebbero soltanto avere il diritto di opporsi agevolmente al trattamento per finalità di commercializzazione diretta, ma anche avere il diritto di farlo "gratuitamente". Questo termine è utilizzato anche all'articolo 16, paragrafo 2, del proposto regolamento, tuttavia soltanto in relazione alla possibilità di opporsi alla commercializzazione diretta sulla base dei dati di contatto ottenuti nel contesto di una vendita.

L'articolo 7, paragrafo 3, del regolamento generale sulla protezione dei dati prevede che revocare il consenso debba essere possibile in qualsiasi momento con la stessa facilità con cui è stato accordato. Inoltre, nel suo parere 4/2010 sulla FEDMA (WP174), il Gruppo di lavoro ha già riconosciuto l'importanza di offrire "un modo semplice, efficace, gratuito, diretto e facilmente accessibile per disisciversi" dalla commercializzazione diretta<sup>18</sup>. Questa norma per la revoca del consenso dovrebbe essere integrata nelle norme per la commercializzazione diretta contenute nel proposto regolamento. Lo stesso dicasi per il requisito di cui all'articolo 7, paragrafo 3, del regolamento generale sulla protezione dei dati, che prevede che la revoca del consenso dovrebbe essere possibile con la stessa facilità con cui è accordato.

29. In relazione a questo aspetto, **si dovrebbero chiarire le modalità per la revoca del consenso o per opporsi alle chiamate di commercializzazione diretta**. A norma dell'articolo 16, paragrafo 4, del proposto regolamento, gli Stati membri sono liberi di scegliere un regime per l'espressione dell'obiezione alle chiamate di commercializzazione vocali. Il regolamento sulla vita privata e le comunicazioni elettroniche dovrebbe specificare le modalità per la revoca del consenso e per opporsi alle chiamate di commercializzazione. Il considerando 36 specifica che gli Stati membri *dovrebbero essere in grado di* istituire e/o mantenere sistemi nazionali per la gestione delle obiezioni. Ai sensi di questa disposizione, gli Stati membri potrebbero quindi persino consentire una situazione nella quale un utente debba esprimere un'obiezione nei confronti di singoli fornitori di comunicazione. Una tale attuazione non tutela gli utenti contro il fastidio generato dalla comunicazione ingiustificata<sup>19</sup> o non mette a disposizione un meccanismo conforme al regolamento generale sulla protezione dei dati per revocare agevolmente il consenso in qualsiasi momento. Di conseguenza il regolamento dovrebbe precisare che ciascuno Stato membro *deve* creare un registro nazionale degli utenti che si oppongono alla ricezione di chiamate di commercializzazione diretta (registro dei numeri da non chiamare). Inoltre, il regolamento dovrebbe specificare che ai destinatari delle chiamate vocali dovrebbero

---

<sup>18</sup> Gruppo di lavoro Articolo 29, WP174, Parere 4/2010 sul codice di condotta europeo della FEDMA per l'utilizzazione dei dati personali nel marketing diretto, adottato il 13 luglio, URL: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174\\_it.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174_it.pdf).

<sup>19</sup> Ad esempio, nel Regno Unito, l'operatore di telefonia BT ha registrato 31 milioni di chiamate importune in una settimana. Cfr. (in inglese): <http://www.bbc.com/news/business-38635921>.

essere date due opzioni per revocare il loro consenso: nei confronti delle chiamate future provenienti da quella specifica impresa od organizzazione e disponendo della possibilità, durante queste chiamate, di registrarsi in un registro nazionale dei numeri da non chiamare.

30. Un altro aspetto che desta preoccupazioni è il fatto che **l'uso di false identità per l'invio di comunicazioni di commercializzazione diretta non è esplicitamente vietato**. Al considerando 34 si afferma che è proibito "l'occultamento dell'identità, gli indirizzi o i numeri di risposta falsi allorché sono inviati messaggi commerciali indesiderati a scopi di commercializzazione diretta". Tuttavia, l'articolo 16, paragrafo 4, afferma semplicemente che gli utenti finali devono essere informati "dell'identità della persona giuridica o fisica per conto della quale è trasmessa la comunicazione". Questo obbligo di informare i destinatari in merito all'identità dovrebbe essere integrato con un chiaro divieto a utilizzare indirizzi di contatto occultati o falsi per scopi di commercializzazione diretta.
31. Questo aspetto si collega a un altro aspetto che desta preoccupazione: **l'obbligo dell'uso di un prefisso specifico per le chiamate di commercializzazione diretta è presentato come un'alternativa all'obbligo di identificazione della linea dalla quale viene effettuato il contatto**. A norma dell'articolo 16, paragrafo 3, le chiamate di commercializzazione diretta sono consentite se il chiamante: i) presenta l'identità di una linea alla quale è possibile contattare la persona fisica o giuridica che effettua la chiamata (articolo 16, paragrafo 3, lettera a)); oppure ii) utilizza un codice o prefisso specifico che consente di identificare la chiamata come una chiamata a fini commerciali (articolo 16, paragrafo 3, lettera b)). Sebbene il Gruppo di lavoro accolga con favore l'obbligo di cui all'articolo 16, paragrafo 3, lettera b) di utilizzare un prefisso, ritiene che tale requisito non risolva la stessa questione affrontata dall'obbligo di identificazione della linea di contatto di cui all'articolo 16, paragrafo 3, lettera a). Mentre il requisito del prefisso intende consentire al destinatario di identificare una chiamata anticipatamente come una chiamata di commercializzazione (e di attuare misure per bloccare tali chiamate), il requisito relativo all'identificazione della linea di contatto è inteso fornire ai destinatari (e alle autorità di controllo) i mezzi per identificare e contattare l'istigatore della comunicazione di commercializzazione. Ciò è particolarmente importante per le chiamate automatiche nell'ambito delle quali vi è un forte squilibrio tra le possibilità del venditore di inviare chiamate importune e le possibilità del destinatario di evitare queste chiamate. Di conseguenza questi due requisiti non devono costituire alternative reciproche, bensì essere complementari tra di loro.

#### *CALENDARIO*

32. Il Gruppo di lavoro Articolo 29 esprime il proprio apprezzamento alla Commissione europea per aver riconosciuto la necessità che il proposto regolamento entri in vigore unitamente al regolamento generale sulla protezione dei dati nel maggio 2018, al fine di evitare incongruenze tra i due atti legislativi. Tuttavia preoccupa comunque il fatto che si tratti di una scadenza ambiziosa che richiede anche la finalizzazione del progetto di codice europeo delle comunicazioni elettroniche. Di conseguenza il

Gruppo di lavoro invita tutte le parti interessate nel processo legislativo a impegnarsi a rispettare la scadenza del maggio 2018.

#### *ULTERIORI PREOCCUPAZIONI*

Questa sezione descrive una serie di ulteriori preoccupazioni.

33. In primo luogo, il Gruppo di lavoro esprime preoccupazione in merito al **suggerimento secondo il quale misure di conservazione dei dati non mirate siano accettabili**. La relazione della proposta di regolamento osserva che, nel quadro del proposto regolamento, gli Stati membri sono liberi di mantenere o creare quadri di riferimento nazionali in materia di conservazione dei dati che prevedano fra l'altro misure di conservazione mirate (par. 1.3). In seguito alla decisione *Tele2/Watson*<sup>20</sup>, è chiaro che i quadri in materia di conservazione che si discostano dalla conservazione mirata non sono consentiti a norma della Carta (e anche in tal caso sono soggetti a importanti condizioni come ad esempio la vigilanza) e che l'accesso in maniera generalizzata ai metadati dovrà essere considerato una violazione del contenuto essenziale dell'articolo 7 analogamente a quanto avviene per l'accesso in maniera generalizzata ai contenuti delle comunicazioni elettroniche (cfr. sentenza della Corte, Schrems e il considerando 94). La formulazione di questa frase suggerisce pertanto che vi possa essere un certo margine per gli Stati membri in merito alle misure di conservazione dei dati che invece non esiste. Un aspetto correlato a ciò è il fatto che **i metadati non beneficiano di un livello di protezione sufficiente** a norma del proposto regolamento. Come osservato al punto 10, il Gruppo di lavoro accoglie con favore il riconoscimento del fatto che i metadati possono rivelare dati estremamente sensibili. Tuttavia, nel contesto del proposto regolamento ai metadati non è accordata la protezione che dovrebbe derivare da tale riconoscimento. Data la sensibilità dei metadati, in particolare, prima di un'analisi a norma dell'articolo 6, paragrafo 2, lettera c), si dovrebbe svolgere una valutazione d'impatto sulla protezione dei dati (cfr. anche l'osservazione al punto 46).
34. In secondo luogo, **il proposto regolamento amplierebbe in maniera non auspicabile le possibilità di conservazione dei dati**. L'articolo 11 del proposto regolamento fa riferimento all'articolo 23, paragrafo 1, lettere da a) a e), del regolamento generale sulla protezione dei dati, nel descrivere le finalità per le quali gli Stati membri possono limitare gli obblighi e i diritti di cui agli articoli da 5 a 8 del regolamento. Il regolamento generale sulla protezione dei dati non prevede tali restrizioni in merito alle categorie particolari di dati, in linea con i rischi elevati per gli interessati. Sebbene l'articolo 15 della direttiva relativa alla vita privata e alle comunicazioni elettroniche consenta attualmente una restrizione analoga, le finalità sono più limitate. Il nuovo regolamento proposto renderebbe possibili nuove restrizioni per finalità di "esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica" (articolo 23, paragrafo 1, lettera d), del regolamento generale sulla protezione dei dati) e "altri importanti obiettivi di

---

<sup>20</sup> ECLI:EU:C:2016:970, URL: <http://curia.europa.eu/juris/celex.jsf?celex=62015CJ0203>.

interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale" (articolo 23, paragrafo 1, lettera e), del regolamento generale sulla protezione dei dati). Queste finalità non sono soltanto nuove rispetto alla direttiva relativa alla vita privata e alle comunicazioni elettroniche, l'ultima finalità di cui all'articolo 23, paragrafo 1, lettera d), e l'intera finalità dell'articolo 23, paragrafo 1, lettera e), sono formulate in maniera estremamente ampia. Di conseguenza si suggerisce di eliminare il riferimento all'articolo 23, paragrafo 1, lettere da a) a e), del regolamento generale sulla protezione dei dati e di menzionare invece soltanto le finalità attualmente menzionate dall'articolo 15 della direttiva relativa alla vita privata e alle comunicazioni elettroniche.

35. **L'obbligo di informare gli utenti in merito ai rischi relativi alla sicurezza ha un ambito di applicazione minimale.** Il Gruppo di lavoro accoglie con favore il fatto che i fornitori di servizi debbano informare gli utenti in merito ai rischi relativi alla sicurezza e alle misure adottate per affrontare tali rischi, quali ad esempio la crittografia (articolo 17 e considerando 37). Tuttavia, il titolo della disposizione recita: "Informazioni sui rischi relativi alla sicurezza rilevati". Il fatto che il titolo menzioni rischi rilevati suggerisce che questa disposizione riguardi esclusivamente violazioni (potenziali) della sicurezza, mentre la formulazione della disposizione e il considerando si concentrano maggiormente sull'educazione generale degli utenti finali. Ad esempio, se un fornitore di servizi rileva che il dispositivo di un utente è infetto da malware ed è diventato parte di una rete di zombie (*botnet*), questa disposizione sembra porre in capo a detto fornitore l'obbligo diretto di informare l'utente in merito ai rischi che ne derivano. Tuttavia, si potrebbe chiarire l'ambito di applicazione di questa disposizione, che non dovrebbe essere limitato a questo scenario specifico. La disposizione dovrebbe coprire almeno i rischi relativi alla sicurezza rilevati in tutte le apparecchiature fornite all'utente finale dal fornitore nel contesto di un abbonamento, come ad esempio i *router* e i dispositivi mobili, nonché l'educazione in merito ai rischi derivanti dalla modifica delle impostazioni impostate in maniera da proteggere la vita privata secondo il principio della tutela della vita privata fin dalla progettazione.

Il Gruppo di lavoro raccomanda di estendere l'ambito di applicazione in maniera da includere i fornitori di programmi che consentono le comunicazioni elettroniche (cfr. considerando 8) ed eventualmente anche una nuova categoria: i fornitori di tecnologia essenziale per garantire la comunicazione, che non sono fornitori di servizi (ad esempio i fornitori di tecnologia di crittografia). Qualora si provvedesse a quest'ultima espansione, occorre prestare attenzione affinché tale obbligo non si sovrapponga agli obblighi di notifica di violazioni della sicurezza previsti in altri strumenti come ad esempio nella direttiva NIS<sup>21</sup> e altri strumenti giuridici relativi ai fornitori di certificati. Poiché quest'ultima categoria di fornitori di tecnologie non ha

---

<sup>21</sup> Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (GU L 194 del 19.7.2016, pag. 1), URL: [http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=urisrv:OJ.L\\_.2016.194.01.0001.01.ITA](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=urisrv:OJ.L_.2016.194.01.0001.01.ITA).

solitamente contatti diretti con gli utenti finali, va spiegato altresì come essi possono rispettare il loro obbligo di informazione a norma di questa disposizione.

36. Il Gruppo di lavoro accoglie con favore le disposizioni di cui agli articoli 2 e 13 che si applicheranno ai servizi di comunicazione interpersonale basata sul numero. Tuttavia, non è immediatamente evidente il motivo per cui un **tale livello di tutela della vita privata non dovrebbe essere disponibile anche per i servizi di chiamata OTT equivalenti sotto il profilo funzionale.**
37. Il Gruppo di lavoro si dice altresì preoccupato per la **mancaanza di chiarezza sul consenso granulare per la ricerca inversa negli elenchi.** L'articolo 15, paragrafo 2, del proposto regolamento, impone ai fornitori di ottenere il consenso dagli utenti finali prima di consentire funzioni di ricerca relative ai dati (cfr. anche il considerando 31). Il Gruppo di lavoro accoglie con favore l'armonizzazione del requisito del consenso per quanto concerne l'inclusione in elenchi, tuttavia si rammarica per la mancanza di granularità in relazione alle diverse tipologie di ricerche. L'attuale direttiva relativa alla vita privata e alle comunicazioni elettroniche consente agli Stati membri di richiedere un requisito di consenso distinto per la ricerca inversa, a norma dell'articolo 12, paragrafo 3. Tale articolo afferma che "[g]li Stati membri possono disporre che sia chiesto il consenso ulteriore degli abbonati per tutti gli scopi di un elenco pubblico diversi dalla ricerca di dati su persone sulla base del loro nome e, ove necessario, di un numero minimo di altri elementi di identificazione". In base a tale disposizione, in molti Stati membri è necessario un consenso distinto per le funzionalità di ricerca inversa, tenendo conto dei diversi livelli di identificabilità e quindi dell'intrusività delle due funzionalità.
38. Da un punto di vista più formale, **il livello delle sanzioni pecuniarie non è armonizzato per tutte le violazioni del regolamento.** Nel proposto regolamento, gli Stati membri stabiliscono le norme relative alle sanzioni per violazioni dell'articolo 23, paragrafo 4, dell'articolo 23, paragrafo 6 e dell'articolo 24 del medesimo regolamento. È più coerente procedere in tal senso anche nel regolamento sulla vita privata e le comunicazioni elettroniche stesso.
39. Infine, **il proposto regolamento si basa su definizioni che possono diventare "bersagli mobili".** Per una serie di concetti chiave, il proposto regolamento fa riferimento a uno strumento giuridico distinto che è attualmente in fase di progetto: la proposta di codice europeo delle comunicazioni elettroniche (cfr. ad esempio l'articolo 4, paragrafo 1, lettera b)). Due importanti esempi a tale proposito sono la definizione di "utente finale", che attualmente comprende persone fisiche e giuridiche, e le definizioni di "servizio di comunicazione elettronica" e "servizio di comunicazione interpersonale", che si riflettono nel proposto regolamento all'articolo 4, paragrafo 1, lettera b); inoltre, l'ultimo termine menzionato è ulteriormente specificato all'articolo 4, paragrafo 2, al fine di includere i tipi di servizi esplicitamente esclusi nel codice europeo delle comunicazioni elettroniche<sup>22</sup>. Il

---

<sup>22</sup> Ad esempio, l'articolo 4, paragrafo 2, del proposto regolamento, afferma che un 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"; mentre l'articolo 2,

presente parere si basa sulle definizioni in vigore attualmente, tuttavia è abbastanza probabile che la proposta di codice europeo delle comunicazioni elettroniche e/o i suoi concetti chiave cambieranno. Ciò avrebbe implicazioni immediate anche per il regolamento sulla vita privata e le comunicazioni elettroniche. Idealmente, tutti i termini che derivano dal codice europeo delle comunicazioni elettroniche dovrebbero essere definiti in maniera indipendente nel contesto del regolamento sulla vita privata e le comunicazioni elettroniche; oppure, quanto meno, il proposto regolamento dovrebbe includere chiarimenti qualora vi siano termini le cui definizioni si discostano rispetto a quelle contenute nel codice europeo delle comunicazioni elettroniche (ad esempio, la suddetta inclusione di "servizi accessori" nella definizione di "servizio di comunicazione interpersonale"). Tuttavia, qualora ciò non fosse possibile, il Gruppo di lavoro desidera suggerire a tutte le parti coinvolte nel processo legislativo di garantire che sia il proposto regolamento sia il codice europeo delle comunicazioni elettroniche siano discussi e votati contemporaneamente, al fine di consentire alle parti interessate di valutare correttamente l'ambito di applicazione e le implicazioni dei nuovi strumenti.

## **5. SUGGERIMENTI PER CHIARIMENTI AL FINE DI GARANTIRE LA CERTEZZA DEL DIRITTO**

Oltre agli aspetti discussi nelle sezioni precedenti, il Gruppo di lavoro desidera sottolineare alcune disposizioni del proposto regolamento che sarebbe necessario chiarire. Tali chiarimenti sono considerati necessari per migliorare la certezza del diritto per tutte le parti interessate affinché il regolamento sulla vita privata e le comunicazioni elettroniche sia inteso e applicato in modo uniforme in tutta l'UE.

### *CHIARIMENTI IN MERITO ALL'AMBITO DI APPLICAZIONE*

40. Per quanto riguarda l'ambito di applicazione del proposto regolamento, il Gruppo di lavoro suggerisce i chiarimenti riportati in appresso.

- a. **Il termine "utente finale" dovrebbe includere tutti i singoli utenti.** L'articolo 2, paragrafo 14, del codice europeo delle comunicazioni elettroniche definisce "utente finale" come un utente che non fornisce reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico. Dovrebbe essere chiarito che le persone che contribuiscono a reti, ad esempio a reti a maglia con il loro router WiFi, non sono escluse dalla portata della protezione del proposto regolamento.
- b. **Dovrebbe essere chiarito che l'ambito di applicazione si estende a tutti gli utenti finali nell'Unione.** L'articolo 3, paragrafo 1, lettera a), prevede che il proposto regolamento si applichi alla fornitura di servizi di comunicazione elettronica a utenti finali "nell'Unione", mentre l'articolo 3, paragrafo 1, lettera c), prevede che essa si applichi alla tutela delle apparecchiature

---

paragrafo 5, del codice europeo delle comunicazioni elettroniche esclude espressamente tali servizi da tale definizione. (All'articolo 2, paragrafo 4, il codice europeo delle comunicazioni elettroniche include il "servizio di comunicazione interpersonale" all'interno della categoria più ampia "servizio di comunicazione elettronica").

terminali degli utenti finali" "ubicati nell'Unione" (sottolineatura aggiunta). Questo punto differisce nelle varie traduzioni. La traduzione tedesca non contiene tale distinzione, mentre altre, come quella francese, spagnola e olandese, la contengono. Dal considerando 9 risulta evidente che l'ambito di applicazione che l'ambito di applicazione è inteso essere ampio, indipendentemente dal fatto che i servizi siano forniti dall'esterno dell'Unione o che il trattamento avvenga nell'Unione o no. Di conseguenza si suggerisce di rimuovere il termine "ubicati" dall'articolo 3, paragrafo 1, lettera c), al fine di sottolineare questo ampio ambito di applicazione.

- c. **Il proposto regolamento sembra proteggere soltanto le comunicazioni riservate *in transit* e non una volta archiviate.** L'approccio attuale adottato nel proposto regolamento consiste nel concentrarsi sulla protezione della trasmissione delle comunicazioni. Si veda ad esempio il considerando 15 secondo il quale si dovrebbe applicare il divieto di intercettazione dei dati delle comunicazioni durante la loro trasmissione, ossia fino alla ricezione del contenuto della comunicazione elettronica da parte del destinatario previsto. L'ambito di applicazione di questa protezione si basa su un quadro concettuale delle comunicazioni che è obsoleto. La maggior parte dei dati delle comunicazioni rimane archiviata presso i fornitori di servizi, anche dopo la ricezione. Occorre garantire che la riservatezza di tali dati rimanga protetta. Inoltre, la comunicazione tra abbonati degli stessi servizi basati su *cloud* (ad esempio i fornitori di posta elettronica) comporterà spesso soltanto una comunicazione molto limitata: l'invio di un messaggio di posta elettronica comporterà per lo più il riflettere lo stesso nella banca dati del fornitore, piuttosto che l'invio effettivo di comunicazioni tra due parti. L'argomentazione secondo la quale tale aspetto sarebbe già trattato dal regolamento generale sulla protezione dei dati non è convincente: l'intento generale del proposto regolamento è proteggere tutte le comunicazioni riservate, indipendentemente dai mezzi tecnici di tale comunicazione. È possibile che si tratti di un mero errore di stesura, in quanto il divieto di cui all'articolo 5 fa riferimento a "conservazione" e "trattamento".
- d. **Tutti gli hotspot pubblici Internet senza fili dovrebbero rientrare nell'ambito di applicazione.** Poiché l'uso di *hotspot* senza fili (*wireless*) è comune, è del tutto logico che non ci sia dubbio sul fatto che la riservatezza delle comunicazioni trasmesse tramite tali hotspot debba essere protetta. Il tentativo del regolamento di chiarire questo aspetto, tuttavia, fallisce poiché l'ambito è esteso soltanto alle reti fornite a un "gruppo indefinito di utenti finali" (considerando 13). Occorre definire i termini "gruppo indefinito di utenti finali" e "gruppo chiuso di utenti finali". In particolare, sarebbe opportuno chiarire che anche le reti senza fili sicure (ossia protette da password) rientrano nell'ambito di applicazione, qualora tale password sia fornita a un gruppo teoricamente indefinito di utenti, la cui identità non può essere determinata anticipatamente (ad esempio i clienti di un caffè o i visitatori di un aeroporto). In questo contesto il principio di fondo è che, in linea con il precedente parere del Gruppo di lavoro sulla revisione della direttiva relativa alla vita privata e alle comunicazioni elettroniche, "*possono essere esentati dallo strumento relativo alla vita privata e alle comunicazioni*



*elettroniche solo i servizi che si verificano in una situazione ufficiale o di occupazione, esclusivamente per finalità correlate al lavoro o ufficiali, o di comunicazione tecnica tra enti non pubblici o enti pubblici soltanto al fine di controllare i processi di lavoro o aziendali, nonché l'uso di servizi per finalità esclusivamente domestiche". (pag. 8).*

- e. **I dati raccolti nel corso dell'offerta di servizi radiofonici e televisivi digitali dovrebbero essere inclusi nell'ambito di applicazione del proposto regolamento.** Data la natura sensibile del comportamento di fruizione di questi servizi, in quanto rivela gli interessi personali e le caratteristiche degli spettatori, il regolamento sulla vita privata e le comunicazioni elettroniche dovrebbe specificare (magari mediante un considerando) che l'esclusione dei servizi che forniscono "contenuti trasmessi utilizzando reti di comunicazione elettronica" dalla definizione del "servizio di comunicazione elettronica" non significa che i fornitori di servizi che offrono sia servizi di comunicazione elettronica sia servizi di contenuto non rientrino nell'ambito di applicazione delle disposizioni del regolamento sulla vita privata e le comunicazioni elettroniche che si rivolge ai fornitori di servizi di comunicazione elettronica. Ciò è particolarmente rilevante in quanto la fornitura di servizi che forniscono "contenuti trasmessi utilizzando reti di comunicazione elettronica" è esclusa dalla definizione di "servizio di comunicazione elettronica" di cui alla proposta di codice europeo delle comunicazioni elettroniche (articolo 2, paragrafo 4).
- f. **Solitamente i dati delle comunicazioni sono dati personali.** Nel considerando 4 è indicato che i dati delle comunicazioni possono includere dati personali. Tuttavia, la maggior parte dei dati delle comunicazioni sono dati personali<sup>23</sup> e, in larga misura, si tratta di dati di natura piuttosto intima e sensibile, quindi questa affermazione andrebbe modificata in modo da affermare che solitamente tali dati sono dati personali.
- g. **Le comunicazioni riservate includono i messaggi all'interno di piattaforme.** Il considerando 1 spiega che il principio di riservatezza dovrebbe applicarsi "agli attuali e ai futuri mezzi di comunicazione". Questo considerando continua fornendo un elenco di esempi di tali mezzi, tra cui si annovera la "messaggistica personale attraverso le piattaforme sociali". Probabilmente questo considerando è inteso comprendere i messaggi privati scambiati tra utenti di una rete sociale (ad esempio, Facebook o Twitter) o i messaggi postati su un diario che sono accessibili a un numero finito di persone, tuttavia la formulazione non è sufficientemente chiara.
- h. **Modalità di applicazione del regolamento sulla vita privata e le comunicazioni elettroniche all'interazione da macchina a macchina.** Come indicato al punto 9, il Gruppo di lavoro accoglie con favore l'ampliamento della protezione all'interazione da macchina a macchina. Tuttavia, questo aspetto è menzionato soltanto nel considerando 12 e non in

---

<sup>23</sup> Cfr. ad esempio la sentenza della Corte del 6 novembre 2003, C-101/01, punto 24 (per quanto riguarda un numero di telefono); la sentenza della Corte del 19 ottobre 2016, C-582/14 (*Breyer*), punto 49 (per quanto riguarda gli indirizzi IP dinamici) e la sentenza della Corte del 8 aprile 2014, C-239/12 e C-594/12 (*Digital Rights Ireland*), punti 26-27 (per quanto riguarda la sensibilità dei metadati).

un articolo corrispondente. Questa protezione è auspicabile, in quanto tali comunicazioni contengono spesso informazioni protette dai diritti alla tutela della vita privata. D'altra parte, una categoria ristretta di comunicazioni pure da macchina a macchina dovrebbe essere esentata qualora tali comunicazioni non abbiano alcun impatto sulla vita privata o sulla riservatezza delle comunicazioni, come ad esempio nei casi in cui tale comunicazione avviene per eseguire un protocollo di trasmissione tra elementi di una rete (ad esempio server, *switch*) affinché gli stessi si possano informare reciprocamente sul loro stato di attività.

Un particolare contesto nel quale l'applicazione del regolamento sulla vita privata e le comunicazioni elettroniche richiede chiarimenti è l'area dei sistemi di trasporto intelligenti. Si prevede che i veicoli trasmetteranno continuamente dati contenenti un identificatore unico, via radio. Senza la protezione aggiuntiva nel quadro del regolamento sulla vita privata e le comunicazioni elettroniche in merito ai dati delle comunicazioni, ciò potrebbe portare a un tracciamento continuo delle abitudini di guida, degli itinerari e della velocità dei conducenti. L'articolo 2, paragrafo 1, del regolamento EECS, tuttavia, contiene una nuova definizione ampliata del concetto di reti di comunicazione. Tali reti includono sistemi di trasmissione che non dispongono di una capacità di amministrazione centralizzata e che consentono la trasmissione di segnali via radio. Il considerando 14 del regolamento sulla vita privata e le comunicazioni elettroniche specifica che tali dati sono i dati delle comunicazioni elettroniche. A norma dell'articolo 5 del proposto regolamento, è vietato qualsiasi tipo di intercettazione, monitoraggio o conservazione di tali dati delle comunicazioni, a meno che non si applichi una delle eccezioni. Tuttavia, vi è interesse a trattare questi dati che consentono a oggetti quali autovetture e dispositivi che si guidano da soli di avvertirsi reciprocamente in merito alla loro prossimità o ad altri rischi. Il Gruppo si chiede quindi quale sia l'eccezione applicabile in questo caso. Il consenso degli utenti finali non è un'eccezione fattibile poiché può diventare necessario essere sempre in grado di trattare questi dati. Di conseguenza i fornitori dovrebbero essere in grado di fare affidamento su un'eccezione specifica che consenta a oggetti quali autovetture e dispositivi che si guidano da soli di avvertirsi reciprocamente in merito alla loro prossimità o ad altri rischi.

#### *CHIARIMENTI SUL CONCETTO DI CONSENSO E SULLA SUA APPLICAZIONE*

41. Per quanto riguarda il concetto e l'applicazione del consenso nel proposto regolamento, il Gruppo di lavoro suggerisce i chiarimenti riportati in appresso.

- a. **Modalità di applicazione del concetto di consenso nel contesto delle persone giuridiche.** Il considerando 3 osserva che il regolamento dovrebbe garantire che le disposizioni del regolamento generale sulla protezione dei dati si applichino anche agli utenti finali aventi natura di persone giuridiche. Secondo il considerando, ciò vale anche per la definizione di consenso di cui al regolamento generale sulla protezione dei dati (cfr. anche il considerando

18). Come osservato al punto 13, il Gruppo di lavoro accoglie con favore l'inclusione esplicita delle persone giuridiche nell'ambito di applicazione del regolamento, tuttavia, l'applicazione pratica di questo principio non è chiara. La definizione di consenso di cui al regolamento generale sulla protezione dei dati richiede che esso sia "informato" e che la manifestazione di volontà dell'interessato sia espressa "mediante dichiarazione o azione positiva inequivocabile" (articolo 4, punto 11, del regolamento generale sulla protezione dei dati). Occorre chiarire quando una persona giuridica possa di fatto essere considerata "informata" e quando vi sia una tale espressione di volontà di una persona giuridica.

- b. In questo contesto, è utile sottolineare che nella maggior parte dei casi il datore di lavoro non può prestare il consenso a nome dei dipendenti poiché quando un datore di lavoro chiede il consenso a un dipendente vi è la possibilità che, dato lo squilibrio di potere esistente, un eventuale diniego da parte del dipendente causi a quest'ultimo un pregiudizio reale o potenziale e quindi il consenso prestato dal dipendente non è valido perché non è liberamente concesso<sup>24</sup>. Per quanto riguarda le **imprese che rilasciano dispositivi o apparecchiature a persone fisiche che lavorano per loro, il proposto regolamento non contiene un'eccezione (idonea)** al divieto di interferenza. Un esempio è il caso in cui un datore di lavoro vuole aggiornare un telefono rilasciato dall'impresa oppure offre ai dipendenti auto noleggiate e per scopi amministrativi consenta a un terzo di raccogliere dati relativi alla localizzazione tramite l'unità di bordo dell'auto. In entrambi i casi il datore di lavoro ha un interesse a interferire con questi dispositivi.

Questa interferenza non può essere considerata necessaria per erogare un servizio della società dell'informazione (articolo 8, paragrafo 1, lettera c)) né per misurare il pubblico del web (articolo 8, paragrafo 1, lettera d)). Al fine di rimediare a tale criticità si potrebbe creare una nuova eccezione che includa una situazione nella quale: i) il datore di lavoro fornisce determinate apparecchiature nel contesto di un rapporto di lavoro; ii) il dipendente è l'utente di tale apparecchiatura; e iii) l'interferenza è strettamente necessaria per il funzionamento dell'apparecchiatura da parte del dipendente (il che implica l'applicazione dei principi di proporzionalità e di sussidiarietà per quanto riguarda la raccolta dei dati). Soltanto qualora tali condizioni siano soddisfatte dovrebbe essere possibile per il datore di lavoro interferire con il dispositivo degli utenti finali.

- c. **Miglioramento dei controlli per porre termine alla trasmissione delle chiamate automatiche.** L'articolo 14 fornisce agli utenti finali un controllo importante per porre termine alla trasmissione di chiamate automatiche effettuate da terzi. Questa protezione può essere migliorata ulteriormente imponendo la richiesta di consenso all'utente finale anche per avviare in primo luogo il processo di chiamata automatico.

---

<sup>24</sup> Cfr. il parere 15/2011 sulla definizione di consenso (WP 187), il parere 8/2001 sul trattamento dei dati personali nel contesto lavorativo (WP48) e il nuovo parere sul trattamento dei dati sul posto di lavoro (adottato contemporaneamente al presente parere).

42. Il Gruppo di lavoro suggerisce di chiarire quanto segue in relazione ai dati relativi alla localizzazione e agli altri metadati.

- a. Il significato di **"dati relativi alla localizzazione generati diversi da quelli connessi all'ambito della fornitura di servizi di comunicazione elettronica" di cui al considerando 17 dovrebbe essere chiarito.** Non è chiaro se ciò si riferisca ai dati relativi alla localizzazione raccolti ad esempio attraverso applicazioni che utilizzano i dati ricavati dalla funzionalità GPS presente nei dispositivi intelligenti e/o che generano dati relativi alla localizzazione basati su router WiFi vicini e/o dati relativi alla localizzazione raccolti da assistenti alla navigazione a bordo e/o altre modalità di generazione di dati relativi alla localizzazione. Questa mancanza di chiarezza crea incertezza giuridica in merito all'ambito di applicazione dell'obbligo. In ogni caso, i dati relativi alla localizzazione del dispositivo terminale di una persona fisica sono dati personali e pertanto il trattamento di tali dati è soggetto agli obblighi derivanti dal regolamento generale sulla protezione dei dati.
- b. Si dovrebbe chiarire che **la maggior parte dei trattamenti legittimi di dati relativi alla localizzazione e di altri metadati non richiede un identificativo univoco.** Il considerando 17 menziona le mappe di calore come esempio di usi commerciali dei metadati delle comunicazioni elettroniche da parte dei fornitori di servizi di comunicazione elettronica. Tuttavia, per creare una mappa di calore di base non sono necessari identificatori univoci basta un semplice conteggio statistico. Un altro esempio menzionato nel considerando, l'uso di strutture esistenti e la pressione sulle stesse, può anch'esso essere conteggiato tramite determinati punti di misurazione, ad esempio creando statistiche aggregate sull'utilizzo delle torri di gestione del traffico per fornire un'indicazione della pressione in una ubicazione in un determinato momento nel tempo, senza dover conoscere anche l'identità delle persone connesse.

Inoltre, il considerando menziona come esempio il mostrare i movimenti del traffico in alcune direzioni durante un determinato intervallo di tempo, nell'ambito del quale sarebbe necessario un identificatore univoco per collegare le posizioni delle persone nei diversi intervalli. Con questo esempio, il considerando sembra legittimare l'ulteriore trattamento di questi dati a sostegno delle analisi di "megadati". L'unica condizione prevista dal proposto regolamento per questo tipo di trattamento è l'obbligo di effettuare una valutazione d'impatto sulla protezione dei dati, se il trattamento è *suscettibile di comportare un elevato rischio per i diritti e le libertà delle persone fisiche*. Questa condizione è insufficiente. Inoltre, è contraria anche all'obbligo di cui all'articolo 6 secondo il quale tale tipologia di trattamento può essere svolta soltanto con il consenso degli utenti e soltanto se i dati non possono essere anonimizzati ovvero privati di qualsiasi identificatore univoco. Spesso gli utenti non possono rifiutare la raccolta dei propri dati di geolocalizzazione da parte dei fornitori di servizi di comunicazione elettronica, laddove tale raccolta sia tecnicamente necessaria per fornire la comunicazione all'utente o

laddove tale trattamento sia necessario per fornire il servizio richiesto (ad esempio la navigazione). Nei precedenti pareri, il Gruppo di lavoro ha concluso che tali dati relativi alla localizzazione provenienti da dispositivi intelligenti sono dati personali di natura sensibile e che i vantaggi dell'analisi di questi dati non prevalgono sui diritti degli utenti alla protezione della riservatezza dei metadati delle loro comunicazioni, né prevalgono sui loro diritti generali alla protezione dei dati garantiti dal regolamento generale sulla protezione dei dati. Di conseguenza, il considerando deve quanto meno specificare che i fornitori devono rispettare gli obblighi derivanti dall'articolo 25 del regolamento generale sulla protezione dei dati in caso di ulteriore trattamento dei dati relativi alla localizzazione o di altri metadati. Ciò comporta quanto meno l'adozione delle seguenti misure:

- i) l'uso di pseudonimi temporanei;
- ii) la cancellazione di qualsiasi tabella di ricerca inversa tra questi pseudonimi e i dati di identificazione originali;
- iii) l'aggregazione a un livello in cui i singoli utenti non possono più essere identificati attraverso i loro itinerari particolari;
- v) la cancellazione dei valori estremi in relazione ai quali l'identificazione sarebbe comunque possibile (tutte queste misure devono essere applicate congiuntamente).

Infine, il regolamento sulla vita privata e le comunicazioni elettroniche deve obbligare le parti coinvolte nel trattamento di dati relativi alla localizzazione e di altri metadati a rendere pubblici i loro metodi di anonimizzazione e di ulteriore aggregazione, nel rispetto della segretezza tutelata dalla legge. Ciò consentirebbe sia alle autorità di controllo sia al pubblico in generale di verificare facilmente se il metodo scelto è adeguato.

#### *CHIARIMENTI SULLE COMUNICAZIONI INDESIDERATE*

43. Il Gruppo di lavoro suggerisce di chiarire i seguenti aspetti in merito alle comunicazioni indesiderate.

- a. **La formulazione del divieto di commercializzazione diretta in assenza di consenso.** L'articolo 16, paragrafo 1, del proposto regolamento attualmente rileva che i servizi di comunicazione elettronica "possono" essere utilizzati per inviare comunicazioni di commercializzazione diretta (con il consenso), ma non contiene un divieto esplicito all'invio (all'indirizzamento o alla presentazione) di commercializzazione diretta senza consenso. Ciò è in contrasto con l'approccio adottato nelle altre disposizioni, nelle quali viene innanzitutto formulato un divieto, il quale viene poi seguito da talune eccezioni specifiche. L'attuale formulazione suggerisce un approccio più indulgente (che presumibilmente non è previsto). Il Gruppo di lavoro suggerisce una formulazione leggermente modificata dell'attuale articolo 13, paragrafo 1, della direttiva relativa alla vita privata e alle comunicazioni elettroniche: "l'uso da parte di persone fisiche o giuridiche di servizi di

comunicazione elettronica, ivi incluse le chiamate vocali, i sistemi automatici di chiamata e di comunicazione, compresi i sistemi semiautomatici che connettono la persona chiamata a una persona, un telefax, una posta elettronica o altri usi di servizi di comunicazione elettronica con la finalità di presentare comunicazioni di commercializzazione diretta agli utenti finali può essere consentito soltanto in relazione agli utenti finali che hanno espresso il loro consenso preventivo".

- b. **Ambito di applicazione delle disposizioni in materia di comunicazioni di commercializzazione e chiamate ai contatti esistenti.** L'articolo 16, paragrafo 2, stabilisce che quando una persona ottiene le coordinate elettroniche per la posta elettronica da un cliente esistente, può utilizzare dette coordinate a scopi di commercializzazione diretta di propri prodotti o servizi se ai clienti è offerta in modo chiaro la possibilità di opporsi gratuitamente e agevolmente a tale uso, al momento della raccolta e in ciascun messaggio. Ciò è attualmente limitato ai recapiti commerciali ottenuti "nel contesto della vendita di un prodotto o servizio" e a scopi di ulteriore commercializzazione di propri prodotti o servizi analoghi. Dato che le disposizioni in materia di commercializzazione diretta si applicano parimenti anche alle attività promozionali non commerciali (ad esempio agli organismi di beneficenza o ai partiti politici), questa disposizione dovrebbe essere modificata in maniera tale da applicarsi in egual misura alle organizzazioni non commerciali per contattare i sostenitori precedenti quando promuovono propri obiettivi o ideali analoghi e il medesimo diritto di opposizione dovrebbe essere applicato anche alle chiamate di commercializzazione diretta. Inoltre, dovrebbe essere fissata una scadenza della validità dei "recapiti dei clienti esistenti" nelle comunicazioni elettroniche a scopo commerciale, di beneficenza o politico e tale scadenza dovrebbe applicarsi anche alle chiamate di commercializzazione diretta. Laddove gli Stati membri abbiano optato per un sistema di obiezione contro le chiamate vocali a scopo di commercializzazione, la presenza di una relazione "commerciale esistente con il cliente" ha priorità rispetto alla registrazione in un registro dei numeri da non chiamare. In tali circostanze, gli utenti finali non hanno alcuna possibilità efficace per prevenire le chiamate importune da parte di imprese od organizzazioni con le quali hanno avuto precedenti contatti ma con le quali non intendono più avere relazioni. Di conseguenza, in linea di principio, il regolamento dovrebbe specificare una validità di questa eccezione in caso di "cliente esistente", ad esempio uno o due anni, in relazione alle aspettative legittime degli utenti finali interessati.
- c. **Applicazione delle norme di commercializzazione diretta alle persone giuridiche.** L'articolo 16, paragrafo 5, del proposto regolamento prevede che gli Stati membri assicurino una sufficiente protezione dell'interesse legittimo degli utenti finali che sono persone giuridiche per quanto riguarda le comunicazioni indesiderate. L'articolo 13, paragrafo 5, della presente direttiva relativa alla vita privata e alle comunicazioni elettroniche descrive gli interessi legittimi degli abbonati diversi dalle persone fisiche. Non è chiaro quali sono le implicazioni di questa modifica nella formulazione. Sarebbe opportuno chiarire nei considerando che questa modifica non riflette

l'intenzione di fornire un livello di protezione inferiore. In relazione a ciò, il divieto di commercializzazione diretta senza consenso riguarda gli "utenti finali aventi natura di persone fisiche che hanno espresso il loro consenso" (sottolineatura aggiunta). Sarebbe opportuno chiarire che ciò include le persone fisiche *che lavorano per* persone giuridiche. D'altro canto, il consenso non sarebbe richiesto qualora si contattino persone giuridiche attraverso recapiti generici resi pubblici a tale scopo (ad esempio "info@companyname.eu").

- d. **Applicazione delle norme in materia di commercializzazione diretta a coloro che agiscono in qualità di rappresentanti (politici):** l'articolo 16, così come formulato, può impedire talune comunicazioni inviate a rappresentanti eletti che illustrano aspetti o interessi commerciali. Sarebbe opportuno precisare che il regolamento non impedisce tali comunicazioni.

#### *CHIARIMENTI SULL'APPLICAZIONE DI STRUMENTI IN MATERIA DI DIRITTI FONDAMENTALI*

44. **L'applicazione della Carta e della CEDU alle leggi nazionali in materia di conservazione dei dati** dovrebbe essere chiarita ulteriormente. Il considerando 26 prevede che tutte le misure adottate dagli Stati membri per salvaguardare l'interesse pubblico, come le misure legali di intercettazione, debbano essere conformi alla Carta (oltre che alla CEDU). Ciò è auspicabile, in quanto è in linea con il ragionamento di cui nella sentenza *Tele2/Watson* secondo la quale eventuali eccezioni nazionali alle protezioni in materia di trattamento dei dati garantite dal diritto dell'Unione sono soggette alla Carta (e, di conseguenza, in caso di infrazioni determinate dalle leggi nazionali si può adire la Corte di giustizia dell'Unione europea). Tuttavia l'articolo 11, del proposto regolamento, si limita a constatare che le restrizioni dell'ambito di applicazione degli articoli 5-8 del proposto regolamento devono rispettare l'essenza dei diritti e delle libertà fondamentali e costituire una misura necessaria e proporzionata. In questo punto si dovrebbe includere anche un riferimento esplicito alla Carta e alla CEDU.

45. **La riservatezza delle comunicazioni è tutelata anche dall'articolo 8 della CEDU.** Nel paragrafo 1.1 della relazione e nel considerando 1, si spiega che il proposto regolamento attua l'articolo 7 della Carta. Ciò è ripetuto al considerando 19. Tuttavia, il diritto fondamentale alla riservatezza delle comunicazioni non è protetto soltanto nel contesto di questa disposizione, ma anche a norma dell'articolo 8 della CEDU. L'inclusione di un riferimento esplicito in un articolo del proposto regolamento confermerebbe ulteriormente che qualsiasi giurisprudenza pertinente della Corte europea dei diritti dell'uomo dovrà altresì essere presa in considerazione nella valutazione del regolamento (finale). Comunque, tale riferimento è già incluso nel considerando 20 (relativo alle apparecchiature terminali) e nel considerando 26 (relativo all'intercettazione legale) e ulteriormente sostenuto dalle considerazioni di cui al punto 2.1 della relazione (relativo al rapporto tra la Carta e la CEDU nel contesto delle persone giuridiche), tuttavia in nessuno degli articoli pertinenti, come ad esempio l'articolo 11, paragrafo 1.

46. Sarebbe opportuno chiarire che **gli obblighi del regolamento generale sulla protezione dei dati, come ad esempio quelli in relazione al regime di violazione dei dati e alle valutazioni d'impatto sulla protezione dei dati, rimangono applicabili** quando le parti trattano dati personali nel contesto dei dati delle comunicazioni elettroniche. Poiché al considerando 5 si menziona che il proposto regolamento è una *lex specialis* del regolamento generale sulla protezione dei dati e che il trattamento di dati delle comunicazioni elettroniche dovrebbe essere consentito soltanto in conformità con il proposto regolamento, potrebbe essere messo in discussione il fatto che taluni obblighi a norma del regolamento generale sulla protezione dei dati si applichino anche nel contesto del proposto regolamento. Questa eventualità si verifica in particolare qualora il proposto regolamento possa essere interpretato nel senso di disporre un determinato obbligo, quando anche il regolamento generale sulla protezione dei dati tratta tale tema. Esempi indicativi includono:

- (i) il proposto regolamento impone una certa notifica di rischi relativi alla sicurezza "rilevati" (articolo 17) (cfr. anche l'osservazione al punto 35) ma il regolamento generale sulla protezione dei dati contiene un regime di notifica delle violazioni dei dati (articoli 33 e 34);
- (ii) il proposto regolamento menziona che lo svolgimento di una valutazione d'impatto sulla protezione dei dati e la consultazione dell'autorità di controllo in linea con il regolamento generale sulla protezione dei dati sono obbligatorie in determinate circostanze (considerando 17 e 19 e articolo 6, paragrafo 3, lettera b)), mentre il regolamento generale sulla protezione dei dati stabilisce già quando è necessario effettuare una valutazione d'impatto sulla protezione dei dati e quando è necessaria una consultazione (articoli 35 e 36); e
- (iii) non è stato specificato che se si rispettano le condizioni necessarie di un'eccezione al divieto di trattamento di cui all'articolo 5 del proposto regolamento, si devono comunque rispettare tutti gli obblighi pertinenti a norma del regolamento generale sulla protezione dei dati laddove si tratti di un trattamento di dati personali e qualsiasi altro trattamento è vietato a norma del regolamento generale sulla protezione dei dati. Di conseguenza, sarebbe opportuno chiarire che la prova di compatibilità di cui all'articolo 6, paragrafo 4, del regolamento generale sulla protezione dei dati non si applica;
- (iv) il proposto regolamento sulla vita privata e le comunicazioni elettroniche non prevede meccanismi di certificazione analoghi agli articoli 42 e 43 del regolamento sulla vita privata e le comunicazioni elettroniche. Poiché l'ambito di applicazione dell'articolo 42 del regolamento generale sulla protezione dei dati è limitato, a rigore di termini, all'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al regolamento generale sulla protezione dei dati, si dovrebbe valutare l'opportunità di inserire una disposizione analoga per consentire la certificazione di trattamenti, norme, prodotti o servizi per garantire la loro conformità con il regolamento sulla vita privata e le comunicazioni elettroniche.



Al fine di assicurare che tale mancanza di chiarezza non venga utilizzata come argomento per ridurre il livello di protezione previsto a norma del proposto regolamento, sarebbe opportuno chiarire che in tutti questi casi i titolari del trattamento devono altresì rispettare il regolamento generale sulla protezione dei dati.

47. Inoltre, sarebbe opportuno chiarire che **il requisito relativo alla revoca del consenso si applica anche nel contesto dell'interferenza con le apparecchiature terminali**. L'articolo 8, paragrafo 1, lettera b) del proposto regolamento prevede la possibilità di interferire con le apparecchiature terminali di utenti finali qualora si disponga del loro consenso. L'articolo 9, paragrafo 3, impone che agli utenti finali sia data la possibilità di revocare il loro consenso in qualsiasi momento, tuttavia ciò si applica soltanto al consenso per l'analisi dei metadati e dei contenuti. Sarebbe opportuno chiarire che tale obbligo si estende all'interferenza con le apparecchiature terminali.
48. Un aspetto correlato a questo è il fatto che sarebbe opportuno chiarire che **il promemoria relativo alla possibilità di revocare il consenso si applica anche al consenso conferito tramite le impostazioni del navigatore**. L'articolo 9, paragrafo 3, prevede che si rammenti agli utenti finali, a intervalli periodici di 6 mesi, la possibilità di revocare il loro consenso in qualsiasi momento. Sebbene il Gruppo di lavoro ritenga che le impostazioni generali di navigatori e altri programmi, inclusi i sistemi operativi, le applicazioni e le interfacce software per dispositivi collegati a Internet delle cose (ossia non basate su controlli granulari specifici) non possano costituire una misura valida per conferire il consenso, in quanto le impostazioni generali non sono appropriate per esprimere un consenso specifico a scenari specifici (cfr. osservazione al punto 24), le impostazioni predefinite dovrebbero essere di facile utilizzo (cfr. osservazione al punto 19). Se tale concetto rimane nel proposto regolamento, le impostazioni devono essere sufficientemente granulari da consentire il controllo di tutti i trattamenti di dati ai quali l'utente sta acconsentendo e coprire tutte le funzionalità dell'apparecchiatura che possano portare al trattamento di dati. Inoltre, all'utente finale dovrebbe essere rammentato, almeno a intervalli periodici (di 6 mesi), la possibilità di modificare tali impostazioni.
49. Il Gruppo di lavoro accoglie con favore il fatto che il proposto regolamento impone che i programmi già immessi sul mercato informino gli utenti finali in merito alle loro opzioni per le impostazioni relative alla vita privata (articolo 10). **Tuttavia, non è chiaro come ciò possa essere applicato in maniera efficace ai prodotti preesistenti** e ad altri che non sono più supportati. Inoltre, sarebbe opportuno fornire ulteriori chiarimenti sulle modalità di applicazione di questo obbligo ai programmi aperti (*open source*), sviluppati in maniera aperta e decentrata.
50. Sarebbe opportuno chiarire che **l'offerta della possibilità di bloccare i marcatori (terzi) a norma dell'articolo 10, del proposto regolamento, ha priorità sull'eccezione per la misurazione del pubblico del web** a norma dell'articolo 8, paragrafo 1, lettera d). In altre parole, si potrebbe altrimenti affermare che sebbene un sito web possa impiegare analisi per misurare il pubblico del web a norma dell'articolo 8, paragrafo 1, lettera d), gli utenti dovrebbero comunque avere il diritto di bloccare queste tecnologie di tracciamento nel proprio navigatore.

51. Si **dovrebbe chiarire la definizione di sistemi (semi)automatici di chiamata e comunicazione**. La definizione di questo termine, di cui all'articolo 4, paragrafo 3, lettera h), del proposto regolamento contiene un riferimento al termine stesso nella seconda parte della frase ("comprese le chiamate effettuate mediante sistemi automatici di chiamata e comunicazione che collegano il chiamato a un operatore"). Si suggerisce di eliminare quest'ultima frase dalla definizione e di modificare la definizione di cui all'articolo 4, paragrafo 3, lettera g), in maniera da includere le chiamate effettuate con l'aiuto di sistemi semiautomatici di comunicazione, come ad esempio i *dialer* automatici che connettono la persona chiamata a una persona.
52. Sarebbe opportuno chiarire l'espressione **"informazioni che costituiscono parte dell'abbonamento al servizio"**. Il considerando 14 afferma che 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". Non appare chiaro che cosa si intenda con questa formulazione.
53. Sarebbe opportuno chiarire **l'applicabilità dei meccanismi di coerenza e di cooperazione**. Nel considerando 38 si osserva che il proposto regolamento si fonda sul meccanismo di coerenza del regolamento generale sulla protezione dei dati. Inoltre, l'articolo 18, paragrafo 1, stabilisce che i capi VI e VII del regolamento generale sulla protezione dei dati si applicano *mutatis mutandis*. L'articolo 19 precisa inoltre che il comitato europeo per la protezione dei dati espleta le mansioni di cui all'articolo 70 del regolamento generale sulla protezione dei dati. Sebbene l'applicazione di queste disposizioni sia relativamente chiara, non è possibile che sorgano dubbi in merito all'interpretazione per quanto riguarda i concetti fondamentali dei meccanismi di coerenza e di cooperazione del regolamento generale sulla protezione dei dati. Ad esempio, il meccanismo di autorità capofila si applica nei casi in cui vi sia un "trattamento transfrontaliero" (articolo 56, paragrafo 1, del regolamento generale sulla protezione dei dati): le modalità di applicazione di tale meccanismo rimangono dubbie in caso di interferenza con le apparecchiature terminali o di analisi dei contenuti o dei metadati a norma del proposto regolamento. Di conseguenza si ritiene consigliabile chiarire l'applicazione di questi concetti fondamentali in un considerando e di sottolineare che eventuali questioni residue relative all'applicabilità di questi capi del regolamento generale sulla protezione dei dati nel contesto del proposto regolamento saranno risolti interpretando le disposizioni di questi capi in linea con il loro intento. Inoltre, si consiglia di chiarire che l'articolo 70 si applica *mutatis mutandis* al comitato europeo per la protezione dei dati nel contesto del proposto regolamento (questo aspetto è attualmente assente dal considerando).

\* \* \*