Camera dei deputati
XVII LEGISLATURA

DOCUMENTAZIONE PER LE COMMISSIONI
ESAME DI ATTI E DOCUMENTI DELL'UE

11 maggio 2017 n. 84

Rispetto della vita privata e tutela dei dati personali nelle comunicazioni elettroniche (COM(2017)10)

Tipo di atto	*Proposta di regolamento*
Data di adozione	*10 gennaio 2017*
Base giuridica	*Artt. 16 e 114 del Trattatto sul funzionamento dell'Unione europea*
Settori di intervento	*Eurovoc (II e III livello): protezione della vita privata; protezione del consumatore*
Esame presso le istituzioni dell'UE	*Assegnato alla Commissione LIBE (Libertà civili, giustizia e affari interni) del Parlamento europeo*
Assegnazione	*15 febbraio 2017 – II Commissione Giustizia*
Termine per il controllo di sussidiarietà	*12 aprile 2017*
Segnalazione da parte del Governo	*Si*

FINALITÀ / MOTIVAZIONE

L'attuale direttiva **sulla privacy delle comunicazioni elettroniche** (direttiva *eprivacy* 2002/58/CE, come modificata nel 2006 e nel 2009) è volta ad armonizzare le disposizioni nazionali necessarie per assicurare un livello equivalente di tutela dei diritti e delle libertà fondamentali, in particolare del **diritto alla vita privata** e alla **riservatezza**, con riguardo al **trattamento dei dati personali nel settore delle comunicazioni elettroniche,** e per assicurare la **libera circolazione di tali dati** e delle **apparecchiature** e dei s**ervizi di comunicazione elettronica** all'interno dell'Unione europea.

Si tratta di un complesso articolato di **norme minime** dirette alla protezione di un bene tutelato dalla stessa Carta dei diritti fondamentali dell'Unione europea (art. 7: "Ogni persona ha diritto al **rispetto della propria vita privata e familiare**, del proprio domicilio, e delle **proprie comunicazioni**"), che dall'entrata in vigore del Trattato di Lisbona ha assunto lo stesso carattere vincolante del diritto primario UE. Tale diritto è altresì incluso nella Convenzione europea dei diritti dell'uomo (art. 8).

Al riguardo la Corte di giustizia dell'UE e la Corte europea dei diritti dell'uomo sono concordi nel ritenere che la confidenzialità delle comunicazioni è parte essenziale del diritto alla riservatezza.

La direttiva si affianca agli strumenti di diritto derivato UE volti a garantire la **protezione dei dati di carattere personale** (tutelata dall'articolo 8 della medesima Carta) (*vedi infra*).

La Commissione europea ha recentemente deciso di effettuare una verifica sull'adeguatezza e sull'efficacia della direttiva, concludendo che la disciplina non è più al passo con i **progressi**

tecnologici, in particolare quelli **basati su Internet intesi a consentire comunicazioni interpersonali**, come il **voice over IP** (**VOIP**: telefonate tramite Internet) la **messaggistica istantanea** e i servizi di **posta elettronica basati sulla rete**. Il limite principale emerso nell'ambito di tale valutazione risiede nel fatto che la direttiva riguarda **unicamente** gli operatori di **telecomunicazioni tradizionali**, non essendo invece applicabile agli operatori che offrono i **servizi di comunicazione elettronica** attualmente **più diffusi** (servizi OTT: Over the top) - ad esempio - **WhatsApp**, **Facebook, Messenger**, **Skype**, **Gmail**, e **iMessage**.

Secondo la Commissione europea, alcune disposizioni della direttiva *eprivacy* si sarebbero inoltre rivelate non sufficientemente chiare determinando una **ambiguità di concetti giuridici** tale da compromettere l'**armonizzazione**, ed in definitiva da creare problemi e oneri inutili alle imprese che svolgono attività transfrontaliere (si tratta ad esempio della disciplina intesa a tutelare la **riservatezza delle apparecchiature terminali**, con particolare riferimento ai **marcatori**, cosiddetti "cookie di tracciatura").

L'esigenza di aggiornare il regime di protezione delle comunicazioni elettroniche è inoltre motivata dalla necessità di **allineamento** con le recenti norme varate dall'UE in materia di **protezione dei dati personali**, la cui applicazione è prevista a partire da maggio 2018. Al riguardo si ricorda che la proposta di regolamento in esame viene configurata dalla Commissione europea come ***lex specialis*** **rispetto al regolamento generale protezione dei dati** di cui precisa e integra il contenuto[1].

Nel preambolo della proposta si afferma che la nuova disciplina non abbasserebbe il livello di tutela delle persone fisiche previsto nel regolamento generale sulla protezione dei dati personali.

Tale affermazione non sembra tuttavia condivisa dal Gruppo ex art. 29 della direttiva sulla protezione dei dati personali[2], il quale ha rilevato che in alcune parti la proposta prevede standard di protezione meno elevati, sottolineando altresì la necessità di un maggiore raccordo tra il regime generale sui dati personali e la futura lex specialis sulle comunicazioni elettroniche (vedi infra, nella parte relativa alla protezione informazioni conservate nelle apparecchiature terminali).

La Commissione europea ritiene infine di contribuire con la nuova disciplina alla **crescita più rapida del mercato unico digitale**: la sostituzione della **direttiva *eprivacy* con un regolamento**, atto legislativo europeo **direttamente applicabile agli ordinamenti degli Stati membri** senza necessità di interposizione di norme nazionali, assoggetterebbe gli operatori economici che forniscono servizi in tale settore ad **un unico regime** europeo, eliminando l'**incertezza giuridica** dovuta alle differenti modalità di recepimento dell'attuale direttiva negli ordinamenti nazionali.

---

[1] Si tratta del 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. Il regolamento in sintesi, introduce regole più chiare in materia di informativa e consenso, definisce i limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio di nuovi diritti (ad esempio i diritti alla portabilità e all'oblio), stabilisce criteri per il trasferimento dei dati al di fuori dell'Ue e per i casi di violazione dei dati personali.

Al riguardo la Commissione europea precisa che mentre il regolamento generale sulla protezione dei dati personali garantisce la **tutela dei dati personali**, la disciplina sulla vita privata elettronica garantisce la **riservatezza delle comunicazioni**, **che possono anche contenere dati non personali** e dati connessi a una persona giuridica (compresi segreti di carattere commerciale).

[2] Il Gruppo ex art. 29 è un organismo istituito a livello UE ai sensi dell'attuale vigente direttiva sui dati personali, composto da un rappresentante delle **autorità di protezione dei dati personali designate da ciascuno Stato membro**, dal **GEPD** (**Garante europeo della protezione dei dati**), nonché da un rappresentante della Commissione, al fine di contribuire (attraverso varie funzioni) alla **applicazione omogenea della disciplina in materia di protezione dei dati personali**. Con l'entrata in vigore del regolamento generale sulla protezione (abrogativo della direttiva citata) in sostanza le funzioni del Gruppo, che cambierebbe nome in Comitato europeo per la protezione dei dati, dovrebbero essere rafforzate.

Quest'ultimo profilo è in linea con la "**Strategia per il mercato unico digitale in Europa**", presentata dalla Commissione europea nel maggio 2015, tra i cui pilastri si annovera la creazione di "un **contesto favorevole** in cui le reti e i servizi digitali possano svilupparsi, caratterizzato da infrastrutture e **servizi ad alta velocità protetti e affidabil**i, in cui siano garantite la concorrenza leale e la parità di condizioni", e che in tale ambito prevede, tra l'altro, azioni volte ad **aumentare fiducia e sicurezza nei servizi digitali** e nella **gestione dei dati personali**.

Il lavoro istruttorio della Commissione europea propedeutico alla presentazione della proposta ha, tra l'altro, incluso:

- una **consultazione pubblica** tra il 12 aprile e il 5 luglio 2016 cui hanno partecipato, tramite 421 contributi, cittadini (società civile e organizzazioni dei consumatori), nonché operatori economici e autorità pubbliche, comprese le autorità responsabili dell'applicazione della direttiva e privacy (si veda, in particolare, la nota del Garante europeo per la protezione dei dati personali del 22 luglio 2016);
- un'**indagine di Eurobarometro** sulla vita privata elettronica, effettuata nel luglio 2016 tramite l'intervista di circa 27 mila cittadini appartenenti a gruppi demograficamente e socialmente differenti.

  In particolare, secondo Eurobarometro:

  - per il 78 per cento degli intervistati è molto importante che l'**accesso alle informazioni personali** contenute nel computer, nel cellulare o nel tablet sia **subordinato al consenso**;
  - il 72 per cento ritiene molto importante che sia garantita la **riservatezza della posta elettronica** e della **messaggistica istantanea** in linea;
  - l'89 per cento concorda con l'opzione suggerita dalla Commissione, ossia che **le impostazioni predefinite** del loro navigatore prevedano il **rifiuto della condivisione delle informazioni**.

CONTENUTI

DISPOSIZIONI GENERALI

Il Capo I reca le disposizioni relative all'**oggetto** e **all'ambito di applicazione della disciplina**, nonché le relative **definizion**i, molte delle quali sono allineate a quelle previste da altri strumenti di diritto derivato UE, come ad esempio il regolamento generale sulla protezione dei dati personali.

In particolare, il nuovo regolamento:

- stabilisce norme in materia di tutela dei diritti e delle libertà fondamentali delle **persone fisiche e giuridiche** per quanto attiene alla **fornitura e all'uso di servizi di comunicazione elettronica**, in particolare il diritto al rispetto della **vita privata** e delle **comunicazion**i nonché la **tutela delle persone fisiche in merito al trattamento dei dati personal**i;
- non intende pregiudicare la **libera circolazione dei dati delle comunicazioni elettroniche** e dei **servizi di comunicazione elettronica** nell'Unione, i quali **non sono limitati né proibiti** per motivi connessi al rispetto della vita privata e delle comunicazioni delle persone fisiche e giuridiche nonché la tutela delle persone fisiche per quanto attiene al trattamento dei dati personal;
- **precisa e integra** il regolamento (UE) 2016/679 (**regolamento generale protezione dati personali**) stabilendo norme specifiche.

L'**ambito di applicazione materiale** della disciplina è precisato all'**articolo 2**, dove si fa riferimento al trattamento dei dati delle comunicazioni elettroniche effettuato in relazione alla **fornitura e alla fruizione di servizi di comunicazione elettronica** e alle **informazioni connesse alle apparecchiature terminali degli utenti finali**.

La disciplina si applica altresì a servizi di comunicazione interpersonale e interattiva che costituiscono una caratteristica accessoria intrinsecamente connessa ad altri servizi, come ad esempio quelli forniti dalle *app* di alcuni giochi (**articolo 4, paragrafo 2**).

Da ultimo si ricorda che il preambolo della proposta (**considerando 12**) chiarisce che la tutela della riservatezza riguarda anche la trasmissione delle comunicazioni da macchina a macchina (con particolare riferimento al cosiddetto Internet delle cose).

Sono **escluse** dall'ambito di applicazione del regolamento:

- le attività degli Stati membri relative alle politiche in materia di gestione delle **frontiere esterne**, di **asilo** e **migrazione**;
- i servizi di comunicazione **non accessibili al pubblico**;
- le attività delle autorità competenti ai fini di **prevenzione**, **indagine**, **accertamento perseguimento** di **reati** o esecuzione di **sanzioni penali**, incluse la salvaguardia contro **minacce alla sicurezza pubblica** e la **prevenzione** delle stesse;

- il **trattamento dei dati** delle comunicazioni elettroniche da parte delle Istituzioni, degli organi, e delle Agenzie dell'**Unione europea** (ambito per il quale è in corso di esame una proposta legislativa di riforma ad hoc).

Il regolamento **non pregiudica** infine l'applicazione della direttiva 2000/31/CE sul **commercio elettronico**, né quella della direttiva 2014/53/UE **sulla messa a disposizione sul mercato di apparecchiature radio**.

L'applicazione del regolamento riguarda **gli utenti finali nell'Unione europea** (**articolo 3, paragrafo, 1 lettera a**).

A tal proposito, secondo il **considerando 9** del preambolo, il regolamento dovrebbe applicarsi anche ai dati delle comunicazioni elettroniche elaborati in relazione alla fornitura e alla fruizione dei servizi di comunicazione elettronica nell'Unione, **indipendentemente dal fatto che il trattamento avvenga nell'Unione o no**; inoltre, al fine di non privare gli utenti finali di una tutela efficace, il regolamento dovrebbe applicarsi anche ai dati delle comunicazioni elettroniche elaborati in relazione alla fornitura di servizi di comunicazione elettronica erogati al di fuori dell'Unione a utenti finali nell'Unione.

Qualora il **fornitore** di un servizio di comunicazione elettronica **non sia ubicato nell'Unione,** esso è tenuto a designare per iscritto un **rappresentante nell'Unione**, stabilito in **uno degli Stati membri in cui sono ubicati gli utenti finali** dei servizi di comunicazione elettronica; tale rappresentante ha il potere di rispondere a domande e fornire informazioni, oltre o in vece del fornitore rappresentato, in particolare alle autorità di controllo e agli utenti finali, in merito a tutte le questioni connesse al trattamento dei dati delle comunicazioni elettroniche al fine di garantire la conformità con il presente regolamento.

Al riguardo, sembra utile un approfondimento sull'adeguatezza sotto il profilo dell'efficacia opportunità della scelta di limitare tale obbligo all'istituzione di un unico rappresentante territoriale in uno degli Stati membri in cui sono ubicati gli utenti finali, nonostante tale organismo possa svolgere le attività citate nei confronti di autorità e utenti appartenenti a diversi Stati dell'UE.

La designazione del rappresentante lascia tuttavia **impregiudicate le azioni legali** che possono essere promosse contro **una persona fisica o giuridica che effettua il trattamento dei dati delle comunicazioni elettroniche** in relazione alla fornitura di servizi di comunicazione elettronica erogati **al di fuori dell'Unione verso utenti finali ubicati nell'Unione** (**articolo 3, paragrafo 5**).

Al riguardo, anche alla luce della disposizione ex articolo 3, paragrafo 5, potrebbe risultare opportuno chiarire, onde evitare equivoci in sede interpretativa, se la tutela apprestata dal regolamento possa riguardare anche cittadini dell'UE che al momento della fruizione dei servizi di comunicazione elettronica si trovino al di fuori dei confini dell'Unione.

Il regolamento **recepisce** le definizioni contenute nel **regolamento generale protezione dati personali**; sono altresì indicate, mediante rinvio alla futura direttiva istitutiva del Codice europeo delle comunicazioni elettroniche[3], le definizioni di "**rete di comunicazione elettronica**", "**servizio di comunicazione elettronica**", "**servizio di comunicazione interpersonale**", "**servizio di comunicazione interpersonale basato sul numero**", "**servizio di comunicazione interpersonale indipendente dal numero**", "**utente finale**" e "**chiamata"** (**articolo 4**).

Al riguardo, si segnala che, durante l'audizione presso la Commissione LIBE del Parlamento europeo dell'11 aprile 2017, il Garante europeo dei dati personali, Giovanni Buttarelli, ha espresso riserve sulla scelta di impiegare nella disciplina in esame definizioni oggetto di negoziato nell'ambito dell'iter legislativo del futuro Codice europeo delle comunicazioni elettroniche.

Si segnala, peraltro, che in sede di negoziato relativamente al futuro Codice europeo delle comunicazioni elettroniche si sono registrate difficoltà per quanto riguarda il raggiungimento di una nozione condivisa di servizio di comunicazione elettronica.

Tra le definizioni introdotte dalla proposta si segnala quella relativa ai "**dati delle**

[3]La proposta di direttiva COM(2016)590 che istituisce il Codice europeo delle comunicazioni elettroniche, presentata dalla Commissione europea nell'ottobre 2016, è tuttora all'esame delle Istituzioni legislative europee.

comunicazioni elettroniche" che a sua volta ricomprende:

- **contenuti** delle comunicazioni elettroniche;

  Si tratta dei contenuti scambiati attraverso i servizi di comunicazione elettronica, quali **testo voce**, **video**, **immagini** e **suono** (tali contenuti possono identificarsi con i dati personali in senso stretto, ma possono anche riguardare dati relativi a persone giuridiche o altri dati non personali).

- **metadati** delle comunicazioni elettroniche.

  Sono i dati trattati in una rete di comunicazione elettronica per trasmettere, distribuire o scambiare il contenuto delle comunicazioni elettroniche compresi i dati usati per tracciare e identificare la **fonte** e il **destinatario** di una comunicazione, i dati relativi alla **localizzazione del dispositivo** generati nel contesto della fornitura di servizi di comunicazione elettronica nonché la **data**, **l'ora**, la **durata** e il **tipo di comunicazione**. Si tratta di informazioni molto significative in quanto permettono di ricostruire caratteristiche anche strettamente personali degli utenti finali dei servizi di comunicazione elettronica.

La proposta introduce, infine, una serie di definizioni per quanto riguarda: l'**elenco pubblico** (**elenco di utenti finali** di servizi di comunicazione elettronica), la "**posta elettronica**", le "**comunicazioni di commercializzazione diretta**", le "**chiamate vocali ai fini di commercializzazione diretta**" e i "**sistemi automatici di chiamate e comunicazione**".

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

Il Capo II include le principali disposizioni volte a garantire la **riservatezza delle comunicazioni elettroniche**, nonché quelle recanti i **fini limitati consentiti** e le **condizioni di trattamento** di tali comunicazioni (**articoli 5-7**).

In particolare, il principio generale di riservatezza delle comunicazioni elettroniche è sancito dall'**articolo** 5, che specifica altresì che sono **vietate tutte le interferenze** con i dati delle comunicazioni elettroniche, quali **ascolto**, **registrazione**, **conservazione**, **monitoraggio**, **scansione** o altri tipi di **intercettazione**, **sorveglianza** o **trattamento dei dati** delle comunicazioni elettroniche, da parte di **persone diverse dagli utenti finali**, salve le **fattispecie previste dal regolamento** stesso. Tali eccezioni sono elencate all'articolo 6 della proposta (**trattamento consentito** dei **dati** delle comunicazioni elettroniche). In estrema sintesi, i **contenuti** e i **metadati** delle comunicazioni elettroniche possono essere trattati dai fornitori di reti e di servizi, in primo luogo, se necessario per realizzare la **trasmissione della comunicazione** e per il **mantenimento e il ripristino della sicurezza** delle reti e dei servizi di comunicazione elettronica (o per rilevare problemi nella trasmissione delle stesse), per la durata necessaria a tal fine.

I fornitori di servizi di comunicazione elettronica possono inoltre **trattare i metadati** se:

a) necessario per soddisfare i **requisiti di qualità obbligatori** previsti dalla futura direttiva istitutiva del codice europeo delle comunicazioni elettroniche o del regolamento (UE) 2015/2120 sull'accesso a un'Internet aperta , per la durata necessaria a tal fine; oppure

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

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

Il **trattamento dei contenuti** è invece **consentito** ai fornitori di servizi di comunicazione elettronica solo:

- a fini di erogazione di un **servizio specifico a un utente finale**, se l'utente finale o gli utenti finali **hanno prestato il loro consenso** al trattamento del contenuto delle loro comunicazioni e l'erogazione del servizio non può essere realizzata senza il trattamento di tale contenuto; oppure
- se **tutti gli utenti finali interessati hanno prestato il loro consenso** al trattamento del contenuto delle loro comunicazioni elettroniche per **uno o più fini specificati** che non possono essere realizzati mediante il trattamento anonimizzato delle informazioni e **il fornitore ha consultato l'autorità di**

controllo (secondo le procedure delineate nel regolamento generale protezione dati personali).

Il Garante europeo per la protezione dei dati ritiene che la disciplina sulla protezione della riservatezza dei dati delle comunicazioni elettroniche (in particolare l'articolato sistema di deroghe al divieto di interferenze da parte di persone diverse dagli utenti e alla richiesta del consenso al trattamento) risulti eccessivamente complessa e per questo suscettibile di determinare lacune. I rilievi del Garante riguarderebbero, in particolare, la scelta del legislatore europeo di individuare differenti livelli di confidenzialità (protezione della comunicazione) a seconda che l'oggetto specifico di cui si intende tutelare la riservatezza sia tecnicamente un contenuto (vedi supra, nella parte relativa alle definizioni), o un metadato. La posizione del Garante europeo riflette altresì quella del Gruppo ex art. 29 della direttiva sulla protezione dei dati personali (di cui il Garante europeo è componente), che nel parere del 4 aprile 2017 ha criticato l'approccio della proposta sottolineando che la disciplina avrebbe dovuto prevedere lo stesso livello di protezione per contenuti e metadati, partendo dal divieto esplicito di trattamento di entrambi senza il consenso degli utenti finali.

In **assenza del consenso degli utenti**, fatta salva una serie di ipotesi in cui la conservazione dei dati è permessa, tra l'altro, per motivi di **sicurezza**, di **gestione di pagamenti/fatturazione dei servizi di comunicazione elettronica**), il regolamento **impone** ai fornitori di servizi di comunicazione elettronica **la cancellazione o l'anonimizzazione** dei **contenuti** e dei **metadati** dopo che i destinatari hanno **ricevuto il contenuto** della comunicazione, e una volta che i **metadati non siano più necessari alla trasmissione** (articolo 7).

Si segnala che, nel caso di **trattamento** dei metadati delle comunicazioni elettroniche ai fini di **fatturazione**, la conservazione è consentita fino alla fine del **periodo in cui una fattura può essere legalmente contestata** o un **pagamento può essere preteso**, conformemente al diritto nazionale.

Il Capo II disciplina altresì la protezione delle apparecchiature terminali, sia garantendo l'**integrità delle informazioni** ivi conservate, sia proteggendo le **informazioni provenienti dall'attrezzatura terminale**, in quanto possono consentire l'**identificazione dell'utente finale**.

È anzitutto stabilito il divieto dell'uso delle **capacità di trattamento e conservazione** dell'apparecchiatura terminale, e della **raccolta di informazioni** dall'apparecchiatura terminale degli utenti finali, comprese informazioni relative ai programmi e i componenti, da parte di una parte diversa dall'utente finale, **eccetto che nei seguenti casi**:

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

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

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

(d) se necessario per **misurare il pubblico del web**, purché tale misurazione sia effettuata dal fornitore del servizio della società dell'informazione richiesto dall'utente finale (**articolo 8, par.1**).

Il principio generale contenuto nella disposizione è che nessuno può inserire dati in un dispositivo terminale (pc, smartphone, tablet, etc.) o al contrario prelevare/trattare dati in esso contenuti **senza il consenso dell'utente finale**. Tale principio è riferibile, tra l'altro, alla pratica dei **cookie**[4]**,** sia di **terze parti**, sia (pur con delle deroghe) di **prime parti**, nonché alle **tecniche di tracciatura in genere** (ma il divieto coprirebbe il caricamento da parte di persone diverse dall'utente finale di qualsiasi file, come ad esempio la trasmissione di un virus).

Il principio del consenso dell'utente finale subisce delle **deroghe** qualora l'operazione effettuata da persona diversa dell'utente finale

[4] I cookie sono file installati dai siti web sui quali si naviga (cookie di prime parti) sulle apparecchiature terminali che consentono, tra l'altro, l'autenticazione informatica, il monitoraggio di sessioni, e la memorizzazione di informazioni specifiche relative agli utenti, ivi compresa la profilazione personale di questi ultimi a fini pubblicitari. Di particolare rilievo, ai fini della disciplina in esame, il concetto di cookie di terze parti, ovvero marcatori che sono impostati da un sito web diverso da quello in cui si sta navigando.

sul dispositivo terminale sia funzionale all'**erogazione del servizio richiesto** da quest'ultimo (si pensi, ad esempio ai **cookie di prime parti** che agevolano la navigazione su un siti web consentendo la memorizzazione del cosiddetto "**carrello degli acquisti**", o ai cookie di memorizzazione della **lingua di navigazione**), o ancora sia diretta a consentire ai fornitori di servizi elettronici richiesti dall'utente, **l'analisi statistica degli accessi al relativo sito web**.

Riscrivendo la disciplina, la Commissione europea ha inteso semplificarla, tra l'altro, conformandosi alle indicazioni interpretative (in particolare, in materia di cookie tecnici) fornite dal citato Gruppo ex articolo 29.

È infine previsto il divieto di **raccolta di informazioni** emesse dalla apparecchiatura terminale per **consentire la connessione ad un altro dispositivo** o a un'**apparecchiatura di rete**, eccetto se:

- effettuata esclusivamente al fine di e per il tempo necessario a stabilire una connessione; oppure
- se è visualizzato un **avviso chiaro** e **ben visibile**, inteso a informare almeno delle **modalità**, delle **finalità**, del **responsabile** (e di tutte le informazioni che il responsabile del trattamento è tenuto a fornire all'interessato ai sensi del regolamento generale sulla protezione dei dati), della raccolta di dati personali nonché di ogni **misura a disposizione dell'utente finale dell'apparecchiatura terminale per arrestare o minimizzare tale raccolta**. Tali informazioni possono essere fornite in combinazione con **icone standardizzate** per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme della raccolta.

La disciplina sulla raccolta di informazioni dall'apparecchiatura terminale ai fini di una connessione ad altro dispositivo o ad altra apparecchiatura di rete riguarda in particolare i sistemi di tracciatura di localizzazione di un apparecchio terminale, ed in definitiva consente la registrazione degli spostamenti fisici degli utenti finali (è il caso del WiFi tracking o del Bluetooth tracking), pratica che in alcuni Stati è particolarmente diffusa in centri commerciali e in aeroporti.

Al riguardo si segnala che il Gruppo ex art. 29 citato, nel parere del 4 aprile 2017, ha espresso forte preoccupazione per tale regime, tra l'altro, nella parte in cui sembra consentire la tracciatura di tali movimenti (lesiva della vita privata in quanto in grado di registrare nel tempo l'accesso ripetuto delle persone a luoghi specifici) prescindendo dalla necessità del consenso degli interessati e prevedendo solamente l'obbligo a carico dei fornitori che seguono queste pratiche di affiggere avvisi ben visibili al limitare della zona coperta con i quali si informano gli utenti finali che entrano nella zona delimitata, e della finalità del tracciamento, del nominativo del responsabile e dell'esistenza di eventuali misure a disposizione dell'utente finale per minimizzare o bloccare la raccolta.

Secondo tale organismo i soggetti che raccolgono tali informazioni potrebbero soddisfare tale requisito semplicemente suggerendo agli utenti finali di spegnere i propri dispositivi per evitare di essere fisicamente tracciati.

Il Gruppo ex art. 29 conclude che questo tipo di tracciatura senza consenso dell'utente finale dovrebbe ammettersi in ipotesi molto limitate, ad esempio al solo scopo di conteggiare le persone che si trovano in un determinato luogo (è il caso dei clienti di un determinato negozio all'interno di un centro commerciale) oppure per misurare i tempi di attesa per effettuare controlli di sicurezza (ad esempio in aeroporto). In ogni caso tali dati dovrebbero essere cancellati o anonimizzati una volta raggiunti i fini statistici.

La proposta rinvia al regolamento generale sulla protezione dei dati personali circa la **definizione e le condizioni per la manifestazione del consenso** al trattamento dei dati delle comunicazioni elettroniche[5] (**articolo 9, paragrafo 1**).

Tale consenso più essere **revocato in qualsiasi momento** e la possibilità di revoca deve essere rammentata ogni **sei mesi** finché prosegue il trattamento.

La disposizione precisa tuttavia che il **consenso all'uso delle capacità di trattamento e conservazione dell'apparecchiatura terminale** e **alla raccolta di informazioni**

[5] Ai sensi di tale disciplina si considera consenso qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

relative ai programmi e i componenti degli utenti finali da parte di altri (ad esempio, il **consenso ai cookie**), laddove tecnicamente possibile e praticabile, possa essere **espresso mediante le opportune impostazioni di una applicazione informatica** che consente **l'accesso a Internet** (**consenso via browser**) (**articolo 9**, **paragrafo 2**).

A tal proposito, si potrebbe valutare la coerenza di tale ultima disposizione (prestazione del consenso via browser) rispetto ai requisiti del consenso (in particolare lo standard di specificità) previsti dalla disciplina generale in materia di protezione dei dati personali.

Il Capo II introduce un ulteriore strumento a tutela della privacy dei dispositivi terminali stabilendo che i programmi che consentono le comunicazioni elettroniche, compreso il recupero e la presentazione di informazioni in rete, debbano offrire agli utenti finali l'**opzione di impedire che terzi conservino informazion**i sull'apparecchiatura terminale di un utente finale o **trattino le informazioni già conservate** su detta apparecchiatura (**articolo 10, par 1**).

In altre parole i fornitori di programmi di comunicazione elettronica dovrebbero configurare i software in uso (i browser) in modo da consentire agli utenti finali di **respingere tecniche di tracciamento di terzi** (cookie di prime e terze parti) attraverso menù di **impostazioni predefinite**. In particolare, al **momento dell'installazione** il programma di comunicazione elettronica deve informare l'utente delle impostazioni relative alla vita privata e **per proseguire nell'installazione** deve essere richiesto il **consenso dell'utente ad una data impostazione** (articolo 10, paragrafo 2).

Secondo la Commissione europea (**considerando 23**) attualmente le impostazioni predefinite per i marcatori nella maggior parte dei navigatori sono del tipo "accetta tutti i marcatori". La Commissione europea ritiene che i fornitori di programmi che consentono il recupero e la presentazione di informazioni presenti in rete dovrebbero essere obbligati a configurare il programma affinché esso preveda l'opzione volta a impedire che terzi conservino informazioni sull'apparecchiatura terminale, spesso presentata come "rifiuta tutti i marcatori di terzi". Gli utenti finali dovrebbero avere a disposizione **un insieme di opzioni di impostazione della vita privata comprese fra la più restrittiva** (per es. "non accettare mai marcatori") e **la meno restrittiva** (per es. "accetta sempre i marcatori") e una **posizione intermedia** (per es. "rifiuta i marcatori di terzi" o "accetta solo i marcatori di prima parte"). Tali impostazioni della vita privata dovrebbero essere presentate in modo facilmente visibile e intelligibile.

Tale meccanismo di controllo anticipato del flusso di informazioni da e verso l'apparecchiatura tramite le impostazioni predefinite all'atto di installare i browser, secondo il Gruppo ex articolo 29 citato, non affronta adeguatamente il problema delle tracciature ingiustificate, minando (rispetto ai dati delle comunicazioni elettroniche e dei dispositivi) i principi (recanti standard più elevati di tutela) stabiliti all'articolo 25 del regolamento generale sulla protezione dei dati (Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita). Secondo il Gruppo ex art. 29, il legislatore europeo dovrebbe chiarire la portata dell'articolo 10 stabilendo altresì l'obbligo per i software di guidare gli utenti attraverso i menù di configurazione al fine di discostarsi dalle impostazioni predefinite scelte al momento dell'installazione del programma.

Il Capo II si conclude con la disciplina recante le finalità e le condizioni in cui gli Stati membri possono **restringere le disposizioni illustrate sulla tutela delle comunicazioni e delle informazioni contenute nei dispositivi finali**. In particolare, l'articolo 11 stabilisce che **il diritto** dell'Unione o **dello Stato membro** possano limitare, mediante misure legislative, gli obblighi e i diritti previsti dagli articoli da 5 a 8 del regolamento, qualora la limitazione rispetti l'essenza dei **diritti** e delle **libertà fondamentali** e costituisca **misura necessaria, appropriata e proporzionata** in una società democratica intesa **a salvaguardare**: la **sicurezza nazionale**, la **difesa**, la **sicurezza pubblica**, la prevenzione, l'indagine, l'accertamento e il perseguimento di **reati o l'esecuzione di sanzioni penali**, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica; altri importanti **obiettivi di interesse pubblico generale** dell'Unione o di uno Stato membro, in particolare un **rilevante interesse economico** o **finanziario** dell'Unione o di uno Stato membro, anche in materia **monetaria**, di **bilancio** e **tributaria**, di **sanità pubblica e sicurezza sociale**.

Da ultimo, si ricorda che nel citato parere del Gruppo ex art. 29 si sottolinea la mancanza nella disciplina a tutela della riservatezza delle informazioni contenute nei dispositivi di un esplicito divieto dei tracking walls, pratica con la

quale si nega ad un utente l'accesso ad un sito web o un ad un servizio a meno che l'utente non acconsenta ad esse tracciato su altri siti o servizi.

CONTROLLO DELLE COMUNICAZIONI ELETTRONICHE

Il Capo III disciplina i diritti degli utenti finali a **controllare l'invio e la ricezione di comunicazioni elettroniche** per tutelare la propria vita privata. In sintesi, la proposta prevede:

a) il diritto degli utenti finali di **impedire la presentazione dell'identificazione della linea chiamante** per garantire l'anonimato (**articolo 12**) e le relative **limitazioni** (**articolo 13**);

   È consentito all'utente finale, tra l'altro di impedire la presentazione dell'identificazione della linea chiamante **in uscita e in entrata**, come anche di **rifiutare le chiamate in entrata** la cui **identificazione** della linea chiamante è stata **bloccata**. Le eccezioni alla restrizione dell'identificazione previste dalla proposta riguardano, in linea di massima, le **chiamate a servizi di emergenza**.

   La proposta attribuisce agli Stati membri il compito di definire una disciplina "più specifica" volta a regolare il **superamento della soppressione della presentazione dell'identificazione della linea chiamante** su base temporanea nei casi in cui gli utenti finali richiedano il **tracciamento di chiamate maligne o importune.**

b) obbligo imposto ai fornitori di comunicazione interpersonale basate sul numero pubblicamente disponibile di prevedere la **possibilità di limitare il ricevimento di chiamate indesiderate** (**articolo 14**).

   In particolare, l'utente finale deve poter gratuitamente:

   - bloccare le chiamate in entrata provenienti da **numeri specifici o da fonti anonime**;
   - **porre termine alla trasmissione delle chiamate automatiche** effettuate da terzi verso l'apparecchiatura terminale dell'utente finale.

Il Capo III disciplina altresì le condizioni in base alle quali gli utenti finali possono essere inclusi in elenchi pubblici. In linea di massima occorre il **consenso delle persone fisiche** all'inserimento in tali elenchi di categorie di dati personali, che devono essere altresì **pertinenti ai fini degli elenchi pubblici** dichiarati dai fornitori del servizio. Questi ultimi conferiscono agli utenti finali aventi natura di persone fisiche i **mezzi per accertare, rettificare e cancellare tali dati** (**articolo 15**).

La disposizione prevede altresì mezzi di tutela in caso di inserimento in elenchi pubblici di **dati relativi a persone giuridiche**. In ogni caso la possibilità che gli **utenti finali non siano inclusi** in un elenco pubblico o di accertare, rettificare e cancellare tutti i dati a essi connessi deve essere offerta a **titolo gratuito**.

L'**articolo** 16 regola la materia delle **comunicazioni indesiderate** ai fini di **commercializzazione diretta** (*spamming*). Tali comunicazioni sono ammesse solo **previo consenso** del destinatario.

Inoltre, qualora una persona fisica o giuridica **ottenga l'indirizzo di posta elettronica** di un utente ai fini di vendita di un prodotto o servizio, l'uso di tali coordinate a fini dell'invio di un messaggio di commercializzazione diretta è consentito solo se al cliente è offerta in modo chiaro e distinto la **possibilità di opporsi gratuitamente** e **agevolmente** a tale uso. Il diritto di obiezione è dato al **momento della raccolta** e **ogniqualvolta si invii un messaggio**.

La medesima disposizione obbliga chi usa servizi di comunicazione elettronica per effettuare chiamate di commercializzazione diretta:

- a **presentare l'identità di una linea** alla quale può essere contattato; oppure
- a presentare un **codice o un prefisso specifico** che identifichi il fatto che trattasi di **chiamata a fini commerciali.**

  Alla Commissione europea è conferito il potere di adottare le misure necessarie per specificare il codice o il prefisso che identifica le chiamate commerciali.

Fatto salvo il **principio del consenso** dell'utente finale alle comunicazioni di commercializzazione diretta, la proposta **rimette agli Stati membri** la facoltà di stabilire per legge che l'effettuazione di chiamate di commercializzazione diretta vocali verso utenti finali aventi natura di persone fisiche sia consentita solo nel rispetto degli utenti finali che sono **persone fisiche** che **non hanno espresso la loro obiezione a ricevere tali comunicazioni** (ad esempio mediante l'inserimento dell'utente in un **elenco** di nominativi che non sia possibile contattare).

L'**articolo 17** contempla l'**obbligo** per i fornitori di servizi di comunicazione elettronica di **avvertire gli utenti finali** in caso di rischio particolare suscettibile di compromettere **la sicurezza della rete e dei servizi**.

Qualora il rischio sia al di fuori del campo di applicazione delle misure che devono essere prese dal fornitore di servizio, quest'ultimo comunica agli utenti finali **tutti i possibili rimedi**, compresi i **relativi costi presumibili**.

AUTORITÀ DI CONTROLLO E APPLICAZIONE INDIPENDENTI

Il Capo IV disciplina il controllo e l'applicazione del futuro regolamento. In particolare, considerato il forte nesso tra la tutela dei dati in generale e la sfera della riservatezza delle comunicazioni elettroniche, la **responsabilità del monitoraggio sull'applicazione della nuova disciplina** viene attribuita alle stesse **autorità di controllo** responsabili del **regolamento generale sulla protezione dei dati personal**i (**articolo 18**).

In particolare, si applicano mutatis mutandis, le disposizioni di tale regolamento per quanto riguarda i poteri e i compiti delle Autorità, compresi i meccanismi di cooperazione in esso previsti volti ad assicurare una applicazione coerente della normativa in tutti gli Stati membri.

È tuttavia previsto (paragrafo 2 della medesima disposizione) che tali Autorità di controllo **collaborino**, qualora opportuno, con le **autorità nazionali di regolamentazione** previste dal futuro **Codice europeo delle comunicazioni elettroniche (autorità in materia di comunicazioni)**.

La proposta amplia altresì i poteri del **Comitato europeo per la protezione dei dati** (che, al momento della data di applicazione del regolamento generale sulla protezione dei dati, subentrerà al Gruppo ex art. 29), al quale è affidata la competenza a garantire l'**applicazione coerente** della nuova disciplina (articolo 19).

Oltre ai compiti già previsti dal regolamento generale sulla protezione dei dati, il Comitato deve:

1) fornire **consulenza alla Commissione** in merito a qualsiasi proposta di **modifica** del futuro regolamento *eprivacy*;
2) **esaminare**, di propria iniziativa o su richiesta di uno dei suoi membri o della Commissione, qualsiasi **questione relativa all'applicazione** del regolamento *eprivacy* e pubblicare **linee guida**, **raccomandazioni** e **migliori pratiche** al fine di promuoverne l'applicazione coerente.

Con il regime proposto la Commissione europea ha, per un verso, optato per un'attribuzione inequivoca del controllo sull'applicazione del regolamento in esame agli organismi competenti per la disciplina generale sulla protezione dei dati personali, in vista della costituzione di un complesso organico e coerente di tutte le norme UE in materia di privacy; per altro verso, tale principio è temperato dalla previsione che i Garanti per la protezione dei dati, ove opportuno, collaborino con le autorità nazionali di regolamentazione previste dal futuro Codice europeo delle comunicazioni elettroniche.

Al riguardo si ricorda che l'attuale direttiva *eprivacy*, approvata nell'ambito del pacchetto europeo sulle telecomunicazioni, è oggetto di monitoraggio nei vari Stati membri secondo modelli non uniformi: in alcuni Stati membri (ad esempio l'Italia) tale responsabilità è affidata al Garante per la privacy; in altri ordinamenti nazionali tali competenze sono, talvolta parzialmente, attribuite ad autority responsabili di altri settori, ed in particolare di quello delle comunicazioni.

La proposta prevede, infine, che le disposizioni previste nel regolamento in materia di protezione dei dati per quanto riguarda le **modalità di collaborazione** tra le **autorità competenti** e con la **Commissione europea**, ivi compreso il cosiddetto **meccanismo di coerenza,** siano applicabili anche alle questioni transfrontaliere connesse alla nuova disciplina in materia di comunicazione elettroniche (**articolo 20**).

RICORSI, RESPONSABILITÀ E SANZIONI

Il Capo V disciplina i **rimedi** a disposizione degli utenti finali e le **sanzioni** che possono essere imposte in conseguenza di una **violazione del futuro regolamento**.

Gli utenti finali dei servizi di comunicazione elettronica dispongono anzitutto degli stessi rimedi contemplati dal regolamento generale sulla protezione dei dati personali: diritto di proporre **reclamo a un'autorità di controllo**; diritto di proporre un **ricorso giurisdizionale** effettivo avverso una **decisione** giuridicamente vincolante **dell'autorità di controllo che la riguarda**; diritto a un **ricorso giurisdizionale effettivo** nei confronti del **titolare del trattamento** o del **responsabile del trattamento dei dati**.

È altresì prevista la **tutela** delle persone fisiche o giuridiche **diverse dagli utenti finali** i cui interessi siano stati lesi a causa di una violazione del nuovo regolamento o aventi un **interesse legittimo nella cessazione** o nella **proibizione della violazione** stessa (articolo 21).

Specularmente a quanto previsto nel regime sulla protezione dei dati recentemente approvato, anche la proposta in oggetto prevede un **diritto al risarcimento del danno materiale o immateriale** subito dagli utenti finali di un servizio di comunicazione elettronica in conseguenza di una **violazione del nuovo regolamento** (articolo 22); la disposizione precisa che il **responsabile della violazione** è tenuto a risarcire l'utente **a meno che non dimostri che l'evento dannoso non sia a lui in alcun modo imputabile** (secondo un meccanismo di esonero delle responsabilità già previsto dal regolamento 2016/679 per i **titolari/responsabili del trattamento dei dati personali**).

Il Capo prevede altresì un regime **di sanzioni pecuniarie amministrative** la cui entità varia a seconda del tipo di disposizione regolamentare violata. In particolare, ai sensi dell'articolo 23 della proposta, è prevista una sanzione fino a **10 milioni di euro**, o (in caso di impresa) fino al **2 per cento** del **fatturato mondiale totale annuo** dell'esercizio precedente, se superiore qualora siano violate le disposizioni concernenti:

- gli obblighi relativi alla tutela delle **informazioni conservate nelle apparecchiature** terminali degli utenti finali (art. 8);
- gli obblighi dei fornitori di programmi per quanto riguarda le **impostazioni relative alla vita privata** (art. 10);
- gli obblighi dei **fornitori degli elenchi pubblici** (art 15);
- gli obblighi previsti dalla **normativa sulle comunicazioni indesiderate** (art 16);

Il livello massimo della sanzione **raddoppia** (**20 milioni** di euro o **4 per cento** del fatturato totale mondiale) in caso di violazione: del principio della **riservatezza delle comunicazioni** (art. 5); del **trattamento consentito dei dati** delle comunicazioni elettroniche (art. 6); dei **termini previsti per la cancellazione** (art 7); di **inosservanza di un ordine** da parte di un'autorità di controllo.

La proposta attribuisce agli Stati membri la competenza di stabilire le sanzioni per le violazioni delle altre disposizioni regolamentari; tali sanzioni devono essere **effettive**, **dissuasive** e **proporzionali**.

Appare opportuno valutare se la scelta operata dalla Commissione europea di stabilire i livelli massimi delle ammende possa determinare, per la discrezionalità demandata alle singole autorità dei Paesi membri, significative differenze nella misura delle sanzioni, favorendo comportamenti opportunistici da parte dei soggetti sui quali ricadrebbero gli obblighi previsti dal regolamento.

Peraltro potrebbe risultare utile un approfondimento in sede di negoziato sull'opportunità di stabilire sanzioni così elevate, tali da determinare un forte impatto finanziario sulle imprese fornitrici di servizi di comunicazione elettronica, non sempre riconducibili a gruppi economici di scala mondiale.

BASE GIURIDICA

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

In particolare, l'articolo 16 del TFUE prevede che le Istituzioni legislative europee, secondo la procedura ordinaria, stabiliscano le **norme relative alla protezione delle persone fisiche** con riguardo al trattamento dei **dati di carattere personale** da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le **norme relative alla libera circolazione di tali dati**.

La Commissione europea ritiene che le **comunicazioni elettroniche** che interessano una **persona fisica** debbano considerarsi di norma alla stregua dei **dati personali**; la tutela di tali persone fisiche con riguardo alla riservatezza delle comunicazioni e al trattamento di tali dati dovrebbe pertanto essere basata sull'articolo 16.

L'iniziativa – secondo la Commissione – è altresì conforme all'articolo 114 del TFUE recante il potere legislativo di Parlamento europeo e Consiglio (procedura legislativa ordinaria) in materia di **instaurazione e funzionamento del mercato interno**, con particolare riferimento al **mercato interno per le comunicazioni elettroniche**.

Si ricorda infine che la proposta mira a realizzare il diritto al **rispetto della vita privata e della vita familiare** sancito sia nell'articolo 7 della **Carta dei diritti fondamentali dell'UE**, sia nell'articolo 8 della **Convenzione europea dei diritti dell'uomo**.

Tali principi sono altresì applicabili alle comunicazioni che interessano le **persone giuridiche**, considerato che la giurisprudenza

della Corte di giustizia dell'Unione europea che quella della Corte europea dei diritti dell'uomo ha stabilito che **le attività professionali delle persone giuridiche** non possono essere escluse dalla **tutela dei diritti** garantita dall'articolo 7 della Carta e dell'articolo 8 della CEDU.

VALUTAZIONE D'IMPATTO

VALUTAZIONE DEL GOVERNO

Nella relazione ex articolo 6, comma 4, della legge n. 234 del 2012, inviata alla Camera il 14 marzo 2017, il Governo reca un giudizio complessivamente positivo della nuova disciplina, ritenuta in grado di apportare **significativi vantaggi** (soprattutto in termini di accresciuta **certezza giuridica**) a tutti gli operatori di mercato che utilizzano i servizi di comunicazione elettronica. Secondo il Governo la nuova disciplina richiederebbe un'**armonizzazione della normativa nazionale** in materia di: comunicazioni elettroniche, **contratti del consumatore** (articoli da 1469-bis a 1469-sexies del codice civile), **vendita di cose mobili** (articoli da 1510 a 1519) e **vendita dei beni di consumo** (articoli da 1519-bis a 1519 nonies).

ESAME PRESSO LE ISTITUZIONI DELL'UE

La proposta è stata assegnata alla Commissione per le libertà civili, la giustizia e gli affari interni (*LIBE*) del Parlamento europeo.

ESAME PRESSO ALTRI PARLAMENTI NAZIONALI

Sulla base dei dati forniti dal sito IPEX, l'esame dell'atto risulta concluso da parte del Consiglio federale austriaco, dalle Cortes generales spagnole, dalla Camera e dal Senato della Repubblica ceca, dalla Seimas della Repubblica di Lituania e dal Senato della Romania.

Si segnala, in particolare, che la Commissione Politiche dell'UE Camera dei deputati della Repubblica ceca, il 21 marzo 2017, ha approvato una risoluzione, recante una valutazione sostanzialmente positiva, con la quale si rileva la necessità di una definizione più chiara dell'ambito di applicazione della nuova disciplina rispetto al regolamento generale sulla protezione dei dati personali, alla direttiva sul commercio elettronico e alla proposta di direttiva istitutiva di un Codice per le comunicazioni elettroniche.

Si ricorda infine le Commissioni riunite in materia di politiche dell'UE delle Cortes generales spagnole e la Commissione per gli affari europei dell'Assembleia da Republica del Portogallo hanno approvato risoluzioni nelle quali si ritiene che la proposta rispetta il principio di sussidiarietà.

Il bollettino è stato curato dall'**Ufficio Rapporti con l'Unione europea** (☎ 06 6760.2145 - ✉ cdrue@camera.it)