



**CONSIGLIO  
DELL'UNIONE EUROPEA**

**Bruxelles, 20 novembre 2008 (21.11)  
(OR. fr)**

**15899/08**

---

---

**Fascicolo interistituzionale:  
2007/0248(COD)**

---

---

**TELECOM 203  
MI 460  
COMPET 490  
DATAPROTECT 94  
CONSOM 182  
CODEC 1582**

**RELAZIONE**

---

del: COREPER  
al: CONSIGLIO  
n. prop. Com: 15387/07 TELECOM 151 MI 298 COMPET 392 DATAPROTECT 50  
CONSOM 133 CODEC 1297  
15422/08 TELECOM 186 MI 427 COMPET 456 DATAPROTECT 88 CONSOM  
170 CODEC 1507  
n. doc. prec.: 15106/08 TELECOM 177 MI 415 COMPET 439 DATAPROTECT 81  
CONSOM 165 CODEC 1471

---

Oggetto : Riesame del quadro normativo UE per le reti ed i servizi di comunicazione elettronica  
Proposta di direttiva del Parlamento europeo e del Consiglio recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione per la tutela dei consumatori  
- Accordo politico

---

**I. INTRODUZIONE**

1. Il 13 novembre 2007 la Commissione ha adottato le proposte legislative sul riesame del quadro normativo UE per le reti ed i servizi di comunicazione elettronica, ossia due direttive di modifica e un regolamento. La presente relazione verte sulla cosiddetta "direttiva sui diritti dei cittadini", in particolare la parte che modifica la direttiva 2002/58/CE sulla e-Privacy. La parte che modifica la direttiva 2002/22/CE sul servizio universale sarà esaminata in una relazione distinta (doc. 15896/08).

2. Uno degli obiettivi fondamentali del quadro normativo è promuovere gli interessi dei cittadini dell'UE, tra l'altro assicurando un livello elevato di protezione dei dati personali e della vita privata e assicurando il mantenimento dell'integrità e della sicurezza delle reti di comunicazione pubbliche. L'importanza di questi obiettivi è ulteriormente rafforzata dal numero sempre maggiore delle nuove minacce elettroniche degli ultimi anni, quali virus, spam, software spia e phishing.

La proposta della Commissione inerente alla direttiva sull'e-Privacy riguarda aspetti quali: fare sì che i consumatori siano informati qualora i loro dati personali siano stati compromessi in seguito a una violazione della sicurezza della rete; conferire agli operatori e alle ANR maggiore responsabilità in relazione alla sicurezza e all'integrità di tutte le reti e i servizi di comunicazione elettronica; rafforzare i poteri di attuazione e controllo delle autorità competenti, in particolare nella lotta allo spam; chiarire le modalità di applicazione delle norme UE ai dispositivi di raccolta dei dati e di identificazione che utilizzano le reti pubbliche di comunicazione elettronica.

3. I lavori sotto presidenza slovena sono sfociati in una relazione sullo stato dei lavori sulla quale si è tenuto uno scambio di opinioni il 12 giugno 2008. Durante la presidenza francese la proposta è stata esaminata in ulteriore dettaglio, anche in relazione al parere in prima lettura adottato dal Parlamento europeo il 24 settembre 2008.
4. La Commissione ha adottato la sua proposta modificata a seguito della prima lettura del Parlamento europeo il 6 novembre 2008 (doc. 15422/08).
5. Il Comitato economico e sociale europeo (CESE) ha adottato il parere il 29 maggio 2008 e il Comitato delle regioni (CdR) il 19 giugno 2008.

## **II. RISULTATI DEI LAVORI DEL COREPER**

1. Il testo della proposta di compromesso della presidenza inerente alla direttiva sull'e-privacy è allegato alla presente relazione. Si tratta di una versione consolidata della proposta di direttiva di modifica, basata sui risultati delle discussioni del Coreper il 14 novembre 2008. Il Comitato ha raggiunto un ampio accordo sul testo.
2. Una delegazione soltanto mantiene una riserva sul testo dell'articolo 6, paragrafo 6ter riguardante il trattamento dei dati relativi al traffico.
3. Tutte le delegazioni mantengono riserve linguistiche sul testo, mentre la Commissione si è riservata di prendere posizione sulla proposta di compromesso della presidenza.

## **III. COMPITO DEL CONSIGLIO**

Si invita pertanto il Consiglio a esaminare i punti tuttora in sospeso per pervenire ad un accordo politico. Il testo dovrà quindi essere trasmesso ai giuristi-linguisti per la messa a punto in vista dell'adozione della posizione comune del Consiglio.

**PROPOSTA DI COMPROMESO DELLA PRESIDENZA RELATIVA ALLA  
VERSIONE CONSOLIDATA DELLA PROPOSTA RECANTE MODIFICA DELLA  
DIRETTIVA 2002/58/CE  
(Direttiva relativa alla vita privata)**

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato che istituisce la Comunità europea e in particolare l'articolo 95,

vista la proposta della Commissione,

visto il parere del Comitato economico e sociale,

visto il parere del Comitato delle regioni,

deliberando secondo la procedura di cui all'articolo 251 del trattato,

considerando quanto segue :

*[per i considerando comuni alla presente direttiva e alla direttiva servizio universale, cfr. direttiva servizio universale]*

- (27) *La liberalizzazione dei mercati e delle reti e dei servizi di comunicazione elettronica, unita al rapido progresso tecnologico, ha stimolato la concorrenza e la crescita economica ed ha prodotto una vasta gamma di servizi destinati agli utenti finali, accessibili attraverso le reti pubbliche di comunicazione elettronica. È necessario garantire un pari livello di tutela dei dati personali e della vita privata ai consumatori e agli utenti, indipendentemente dalle tecnologie utilizzate per fornire un determinato servizio.*

**(30 ter) In sede di attuazione delle misure di recepimento della direttiva 2002/58/CE, le autorità e i giudici degli Stati membri dovrebbero non solo interpretare il diritto nazionale in modo conforme a detta direttiva, ma anche provvedere a non fondarsi su un'interpretazione di detta direttiva che entri in conflitto con altri diritti fondamentali o principi generali del diritto comunitario, come il principio di proporzionalità.**

*[per gli altri considerando, cfr. pertinenti articoli]*

HANNO ADOTTATO LA PRESENTE DIRETTIVA:

## *Articolo 1*

### **Finalità e campo d'applicazione**

1. La presente direttiva [...] **prevede l'armonizzazione** delle disposizioni degli Stati membri necessarie per assicurare un livello equivalente di tutela dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata, con riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche e per assicurare la libera circolazione di tali dati e delle apparecchiature e dei servizi di comunicazione elettronica all'interno della Comunità.
2. Ai fini di cui al paragrafo 1, le disposizioni della presente direttiva precisano e integrano la direttiva 95/46/CE. Esse prevedono inoltre la tutela dei legittimi interessi degli abbonati che sono persone giuridiche.
3. La presente direttiva non si applica alle attività che esulano dal campo di applicazione del trattato che istituisce la Comunità europea, quali quelle disciplinate dai titoli V e VI del trattato sull'Unione europea né, comunque, alle attività riguardanti la sicurezza pubblica, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) o alle attività dello Stato in settori che rientrano nel diritto penale.

## *Articolo 2*

### **Definizioni**

Salvo diversa disposizione, ai fini della presente direttiva si applicano le definizioni di cui alla direttiva 95/46/CE e alla direttiva 2002/21/CE [...] che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica (direttiva quadro).

Si applicano inoltre le seguenti definizioni:

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

- (b) "dati relativi al traffico": qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;
- (c) "dati relativi all'ubicazione": ogni dato trattato in una rete di comunicazione elettronica **o da un servizio di comunicazione elettronica** che indichi la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;
- (d) "comunicazione": ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse, come parte di un servizio di radiodiffusione, al pubblico tramite una rete di comunicazione elettronica salvo quando le informazioni possono essere collegate all'abbonato o utente che riceve le informazioni che può essere identificato;
- (e) trasferita nella direttiva quadro*
- (f) "consenso" dell'utente o dell'abbonato: corrisponde al consenso della persona interessata di cui alla direttiva 95/46/CE;
- (g) "servizio a valore aggiunto": il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;
- (h) "posta elettronica": messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente fino a che il ricevente non ne ha preso conoscenza.
- (i) **"violazione dei dati personali": violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di servizi di comunicazione accessibili al pubblico nella Comunità.**

### Articolo 3

#### Servizi interessati

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

2. **Soppresso**

3. **Soppresso**

*(27bis nuovo) In linea con gli obiettivi del quadro normativo UE per la comunicazione elettronica, con i principi di proporzionalità e di sussidiarietà nonché ai fini della certezza del diritto e dell'efficienza nei confronti sia delle imprese europee sia delle autorità nazionali di regolamentazione, la direttiva riguarda le reti o servizi pubblici di comunicazione elettronica e non si applica ai gruppi chiusi di utenti né alle reti aziendali.*

*(28) Il progresso tecnologico permette lo sviluppo di nuove applicazioni basate su dispositivi per la raccolta e l'identificazione dei dati, come ad esempio i dispositivi senza contatto che utilizzano le radiofrequenze. Gli RFID (Radio Frequency Identification Devices, dispositivi di identificazione a radiofrequenza), ad esempio, utilizzano le radiofrequenze per rilevare dati da etichette identificate in modo univoco, che possono in seguito essere trasferiti attraverso le reti di comunicazione esistenti. Un ampio utilizzo di tali tecnologie può generare significativi vantaggi economici e sociali e, di conseguenza, apportare un contributo prezioso al mercato interno, sempre che il loro utilizzo risulti accettabile per la popolazione. A tal fine, è necessario garantire la tutela **di tutti i** diritti fondamentali degli individui, [...] **compreso** il diritto alla vita privata e alla tutela dei dati personali. Quando tali dispositivi sono collegati a reti di comunicazione elettronica accessibili al pubblico, o usano servizi di comunicazione elettronica come infrastruttura di base, è opportuno che si applichino le disposizioni pertinenti della direttiva 2002/58/CE, in particolare quelle sulla sicurezza, sui dati relativi al traffico e alla localizzazione e sulla riservatezza.*

## *Articolo 4*

### **Sicurezza del trattamento**

1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico deve prendere appropriate misure tecniche e organizzative per salvaguardare la sicurezza dei suoi servizi, se necessario congiuntamente con il fornitore della rete pubblica di comunicazione per quanto riguarda la sicurezza della rete. Tenuto conto delle attuali conoscenze in materia e dei loro costi di realizzazione, dette misure assicurano un livello di sicurezza adeguato al rischio esistente.
2. Nel caso in cui esista un particolare rischio di violazione della sicurezza della rete, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico ha l'obbligo di informarne gli abbonati indicando, qualora il rischio sia al di fuori del campo di applicazione delle misure che devono essere prese dal fornitore di servizio, tutti i possibili rimedi, compresi i relativi costi presumibili.
3. **Se si produce una violazione di dati personali [...] il fornitore interessato di servizi di comunicazione elettronica accessibili al pubblico [...] valuta la portata della violazione di dati personali e la relativa gravità ed esamina se sia necessario comunicare detta violazione all'autorità nazionale competente e all'abbonato interessato, tenendo conto delle norme pertinenti fissate dall'autorità nazionale competente in conformità del paragrafo 3bis.**

**Quando la violazione di dati personali rappresenta un grave rischio per la vita privata dell'abbonato, il fornitore interessato di servizi di comunicazione elettronica accessibili al pubblico comunica l'avvenuta violazione all'autorità nazionale competente e all'abbonato interessato senza indugio.**

**La comunicazione all'abbonato contiene almeno una descrizione della natura della violazione di dati personali e i punti di contatto presso cui si possono ottenere maggiori informazioni ed elenca le misure raccomandate per attenuare [...] i possibili effetti negativi della violazione di dati personali. La comunicazione all'autorità nazionale [...] competente descrive, inoltre, le conseguenze della violazione di dati personali e le misure proposte o adottate dal fornitore per porvi rimedio .**

- (28 ter) *È opportuno che il fornitore di un servizio di comunicazione elettronica accessibile al pubblico adotti misure tecniche e organizzative adeguate per assicurare la sicurezza dei suoi servizi. Fatte salve le disposizioni della direttiva 1995/46/CE, tali misure dovrebbero assicurare che i dati personali siano accessibili soltanto al personale autorizzato per scopi legalmente autorizzati e che i dati personali conservati o trasmessi nonché la rete e i servizi siano protetti. Occorre inoltre istituire una politica di sicurezza per il trattamento dei dati personali onde individuare le vulnerabilità del sistema e mettere in atto un monitoraggio regolare e misure di prevenzione, correzione e attenuazione.*
- (28 quater) *È opportuno che le autorità nazionali competenti controllino le misure adottate e diffondano le migliori prassi dei fornitori dei servizi di comunicazione elettronica accessibili al pubblico.*
- (29) *Una violazione di sicurezza che comporti la perdita o il danneggiamento dei dati personali di un abbonato può, se non è trattata in modo adeguato e tempestivo, provocare un grave danno economico e sociale, tra cui l'usurpazione d'identità. Pertanto il fornitore di un servizio di comunicazione elettronica accessibile al pubblico, non appena viene a conoscenza del fatto che si è verificata tale violazione, dovrebbe valutare i rischi che essa comporta, ad esempio determinando il tipo di dati interessati dalla violazione (inclusi il carattere sensibile, il contesto e le misure di sicurezza esistenti), la causa e la portata della violazione della sicurezza, il numero di abbonati interessati e l'eventuale danno per gli abbonati che essa comporta (ad esempio furto d'identità, perdita finanziaria, perdita di opportunità economiche o occupazionali, danni fisici). È opportuno che gli abbonati che sono vittima di [...] violazioni di sicurezza che possono comportare rischi gravi per la loro vita provata (ad esempio il furto o l'usurpazione d'identità, il danno fisico, umiliazione grave o danno alla reputazione) siano informati tempestivamente per permettere loro di adottare le precauzioni necessarie. È opportuno che la comunicazione contenga informazioni sulle misure adottate dal fornitore per affrontare la violazione e raccomandazioni per gli utenti interessati. La comunicazione di una violazione della sicurezza a un abbonato non è necessaria se il fornitore ha dimostrato all'autorità competente di aver utilizzato le opportune misure di protezione tecnologica e che tali misure erano state applicate ai dati interessati dalla violazione della sicurezza. Le misure di protezione tecnologica rendono i dati incomprensibili a chiunque non sia autorizzato ad accedervi.*
- (30) *È necessario che le autorità nazionali di regolamentazione difendano gli interessi dei cittadini dell'Unione europea contribuendo, tra l'altro, ad assicurare un elevato livello di protezione dei dati personali e della vita privata. A tal fine esse devono disporre dei mezzi necessari per svolgere i loro compiti, in particolare di dati completi ed affidabili circa gli incidenti di sicurezza realmente verificatisi che hanno danneggiato i dati personali di singoli abbonati.*

**3bis. Gli Stati membri provvedono affinché l'autorità nazionale competente sia in grado di fissare norme dettagliate e, ove necessario, stabilire istruzioni relative alle circostanze in cui il fornitore di un servizio di comunicazione elettronica accessibile al pubblico ha l'obbligo di comunicare le violazioni di dati personali, al formato applicabile a tale comunicazione, nonché alle relative modalità di effettuazione.**

4. Per assicurare l'attuazione uniforme delle misure di cui ai paragrafi 1, 2, 3 e 3bis, dopo aver consultato l'Agenzia europea per la sicurezza delle reti e dell'informazione, il Gruppo dell'articolo 29 e il Garante europeo della protezione dei dati, la Commissione può adottare [...] raccomandazioni riguardanti, tra l'altro, le circostanze, il formato e le procedure applicabili alle prescrizioni in materia di informazioni e comunicazioni di cui al presente articolo.

[...]

- (31) *Occorre prevedere [...] l'adozione da parte della Commissione di raccomandazioni sui mezzi per conseguire un adeguato livello di protezione della vita privata e di sicurezza dei dati personali trasmessi o trattati in relazione all'uso di reti di comunicazione elettronica nel mercato interno.*
- (32) *Al momento della fissazione delle modalità relative al formato e alle procedure applicabili alla comunicazione delle violazioni [...] di dati personali, occorre tenere debitamente conto delle circostanze della violazione, in particolare del fatto che i dati personali fossero o no protetti mediante cifratura o altri metodi che limitano efficacemente il rischio di usurpazione d'identità o altre forme di abuso. Inoltre, è opportuno che tali norme e procedure tengano conto degli interessi legittimi delle autorità incaricate dell'applicazione della legge, nei casi in cui una diffusione prematura rischi di ostacolare inutilmente l'indagine sulle circostanze di una violazione di sicurezza.*

***Il considerando (33) è soppresso.***

## *Articolo 5*

### **Riservatezza delle comunicazioni**

1. Gli Stati membri assicurano, mediante disposizioni di legge nazionali, la riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, nonché dei relativi dati sul traffico. In particolare essi vietano l'ascolto, la captazione, la memorizzazione e altre forme di intercettazione o di sorveglianza delle comunicazioni, e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza consenso di questi ultimi, eccetto quando sia autorizzato legalmente a norma dell'articolo 15, paragrafo 1. Questo paragrafo non impedisce la memorizzazione tecnica necessaria alla trasmissione della comunicazione fatto salvo il principio della riservatezza.
  
2. Il paragrafo 1 non pregiudica la registrazione legalmente autorizzata di comunicazioni e dei relativi dati sul traffico se effettuata nel quadro di legittime prassi commerciali allo scopo di fornire la prova di una transazione o di una qualsiasi altra comunicazione commerciale.
  
3. Gli Stati membri assicurano che [...] **l'archiviazione di** informazioni [...] **oppure l'accesso a** informazioni **già** archiviate nell'apparecchiatura terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente sia stato informato in modo chiaro e completo, in conformità della direttiva 95/46/CE, tra l'altro sugli scopi del trattamento e che gli sia offerta la possibilità di rifiutare tale trattamento da parte del responsabile del trattamento. Ciò non impedisce l'eventuale memorizzazione tecnica o l'accesso al solo fine di effettuare o facilitare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria a fornire un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente.

- (34) *I software che registrano le azioni dell'utente in modo surrettizio e/o pregiudicano il funzionamento dell'apparecchiatura terminale di un utente a profitto di un terzo (i cosiddetti "software spia" o spyware) costituiscono una grave minaccia per la vita privata degli utenti. Occorre garantire indistintamente a tutti gli utenti un livello elevato di protezione della sfera privata contro tutti i software spia, scaricati inconsapevolmente dalle reti di comunicazione elettronica o installati in modo surrettizio nei software distribuiti su supporti esterni per la memorizzazione dei dati quali CD, CD-ROM o chiavi USB. **Gli Stati membri dovrebbero incoraggiare gli utenti finali ad adottare le misure necessarie per proteggere le loro apparecchiature terminali contro i virus e i software spia.***

## Articolo 6

### Dati sul traffico

1. I dati sul traffico relativi agli abbonati ed agli utenti, trattati e memorizzati dal fornitore di una rete pubblica o di un servizio pubblico di comunicazione elettronica devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione di una comunicazione, fatti salvi i paragrafi 2, 3, [...] 5 e **6bis** del presente articolo e l'articolo 15, paragrafo 1.
2. I dati relativi al traffico che risultano necessari ai fini della fatturazione per l'abbonato e dei pagamenti di interconnessione possono essere sottoposti a trattamento. Tale trattamento è consentito solo sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento.
3. Ai fini della commercializzazione dei servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico ha facoltà di sottoporre a trattamento i dati di cui al paragrafo 1 nella misura e per la durata necessaria per siffatti servizi, o per la commercializzazione, sempre che l'abbonato o l'utente a cui i dati si riferiscono abbia **espresso preliminarmente** il proprio consenso. Gli abbonati o utenti hanno la possibilità di ritirare il loro consenso al trattamento dei dati relativi al traffico in qualsiasi momento.
4. Il fornitore dei servizi deve informare l'abbonato o l'utente sulla natura dei dati relativi al traffico che sono sottoposti a trattamento e sulla durata del trattamento ai fini enunciati al paragrafo 2 e, prima di ottenere il consenso, ai fini enunciati al paragrafo 3.

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

6. I paragrafi 1, 2, 3 e 5 non pregiudicano la facoltà degli organismi competenti di ottenere i dati relativi al traffico in base alla normativa applicabile al fine della risoluzione delle controversie, in particolare di quelle attinenti all'interconnessione e alla fatturazione.

**6 bis. [...] I dati relativi al traffico possono essere trattati [...] nella misura strettamente necessaria [...] ai fini della sicurezza delle reti e dell'informazione, quale definita all'articolo 4, lettera c) del regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione [...].<sup>1</sup>**

*(26 bis) Il trattamento dei dati relativi al traffico nella misura strettamente necessaria per la rilevazione, l'ubicazione e l'eliminazione dei guasti e delle carenze della rete e ai fini della sicurezza dell'informazione, a garanzia della disponibilità, autenticità, integrità e riservatezza dei dati conservati o trasmessi, [...] contribuirà a prevenire l'accesso non autorizzato e la distribuzione dolosa del codice, [...] attacchi finalizzati al diniego di servizi e danni al computer e ai sistemi di comunicazione elettronica. [...]*

---

<sup>1</sup> DE ha espresso una riserva sul paragrafo 6bis.

## *Articolo 7*

### **Fatturazione dettagliata**

1. Gli abbonati hanno diritto di ricevere fatture non dettagliate.
2. Gli Stati membri applicano norme nazionali per conciliare i diritti degli abbonati che ricevono fatture dettagliate con il diritto alla vita privata degli utenti chiamanti e degli abbonati chiamati, ad esempio garantendo che detti utenti e abbonati possano disporre, per le comunicazioni e per i pagamenti, di sufficienti modalità alternative che tutelino maggiormente la vita privata.

## *Articolo 8*

### **Presentazione e restrizione dell'identificazione della linea chiamante e collegata**

1. Qualora sia disponibile la presentazione dell'identificazione della linea chiamante, il fornitore dei servizi deve offrire all'utente chiamante la possibilità di impedire, mediante una funzione semplice e gratuitamente, la presentazione dell'identificazione della linea chiamante, chiamata per chiamata. L'abbonato chiamante deve avere tale possibilità linea per linea.
2. Qualora sia disponibile la presentazione dell'identificazione della linea chiamante, il fornitore di servizi deve offrire all'abbonato chiamato la possibilità, mediante una funzione semplice e gratuitamente, per ogni ragionevole utilizzo di tale funzione, di impedire la presentazione dell'identificazione delle chiamate entranti.
3. Qualora sia disponibile la presentazione dell'identificazione della linea chiamante e tale indicazione avvenga prima che la comunicazione sia stabilita, il fornitore di servizi deve offrire all'abbonato chiamato la possibilità, mediante una funzione semplice, di respingere le chiamate entranti se la presentazione dell'identificazione della linea chiamante è stata eliminata dall'utente o abbonato chiamante.

4. Qualora sia disponibile la presentazione dell'identificazione della linea collegata, il fornitore di servizi deve offrire all'abbonato chiamato la possibilità di impedire, mediante una funzione semplice e gratuitamente, la presentazione dell'identificazione della linea collegata all'utente chiamante.
5. Il paragrafo 1 si applica anche alle chiamate provenienti dalla Comunità e dirette verso paesi terzi. I paragrafi 2, 3 e 4 si applicano anche alle chiamate in entrata provenienti da paesi terzi.
6. Gli Stati membri assicurano che, qualora sia disponibile la presentazione dell'identificazione della linea chiamante o di quella collegata, il fornitore di servizi di comunicazione elettronica accessibili al pubblico informi quest'ultimo di tale possibilità e delle possibilità di cui ai paragrafi 1, 2, 3 e 4.

#### *Articolo 9*

#### **Dati relativi all'ubicazione diversi dai dati relativi al traffico**

1. Se i dati relativi all'ubicazione diversi dai dati relativi al traffico, relativi agli utenti o abbonati di reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico possono essere sottoposti a trattamento, essi possono esserlo soltanto a condizione che siano stati resi anonimi o che l'utente o l'abbonato abbiano dato il loro consenso, e sempre nella misura e per la durata necessaria per la fornitura di un servizio a valore aggiunto. Prima di chiedere il loro consenso, il fornitore del servizio deve informare gli utenti e gli abbonati sulla natura dei dati relativi all'ubicazione diversi dai dati relativi al traffico che saranno sottoposti a trattamento, sugli scopi e sulla durata di quest'ultimo, nonché sull'eventualità che i dati siano trasmessi ad un terzo per la prestazione del servizio a valore aggiunto. Gli utenti e gli abbonati devono avere la possibilità di ritirare il loro consenso al trattamento dei dati relativi all'ubicazione diversi dai dati relativi al traffico in qualsiasi momento.
2. Se hanno dato il consenso al trattamento dei dati relativi all'ubicazione, diversi dai dati relativi al traffico, l'utente e l'abbonato devono continuare ad avere la possibilità di negare, in via temporanea, mediante una funzione semplice e gratuitamente, il trattamento di tali dati per ciascun collegamento alla rete o per ciascuna trasmissione di comunicazioni.

3. Il trattamento dei dati relativi all'ubicazione diversi dai dati relativi al traffico ai sensi di paragrafi 1 e 2 deve essere limitato alle persone che agiscono sotto l'autorità del fornitore della rete pubblica di telecomunicazione o del servizio di comunicazione elettronica accessibile al pubblico o del terzo che fornisce il servizio a valore aggiunto, e deve essere circoscritto a quanto è strettamente necessario per la fornitura di quest'ultimo.

#### *Articolo 10*

##### **Deroghe**

Gli Stati membri assicurano che esistano procedure trasparenti in base alle quali il fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico:

- (a) possa annullare, in via temporanea, la soppressione della presentazione dell'identificazione della linea chiamante a richiesta di un abbonato che chieda la presentazione dell'identificazione di chiamate malintenzionate o importune. In tal caso, in base al diritto nazionale, i dati che identificano l'abbonato chiamante sono memorizzati e resi disponibili dal fornitore di una rete pubblica di comunicazioni e/o di un servizio di comunicazioni elettroniche accessibile al pubblico;
- (b) possa annullare la soppressione della presentazione dell'identificazione della linea chiamante e possa sottoporre a trattamento i dati relativi all'ubicazione, nonostante il rifiuto o il mancato consenso temporanei dell'abbonato o dell'utente, linea per linea, per gli organismi che trattano chiamate di emergenza, riconosciuti come tali da uno Stato membro, in particolare per le forze di polizia, i servizi di ambulanza e i vigili del fuoco, affinché questi possano reagire a tali chiamate.

#### *Articolo 11*

##### **Trasferimento automatico della chiamata**

Gli Stati membri provvedono affinché ciascun abbonato abbia la possibilità, gratuitamente e mediante una funzione semplice, di bloccare il trasferimento automatico delle chiamate verso il proprio terminale da parte di terzi.

## *Articolo 12*

### **Elenchi di abbonati**

1. Gli Stati membri assicurano che gli abbonati siano informati, gratuitamente e prima di essere inseriti nell'elenco, in merito agli scopi degli elenchi cartacei o elettronici a disposizione del pubblico o ottenibili attraverso i servizi che forniscono informazioni sugli elenchi, nei quali possono essere inclusi i loro dati personali, nonché in merito ad ogni ulteriore possibilità di utilizzo basata su funzioni di ricerca incorporate nelle versioni elettroniche degli elenchi stessi.
2. Gli Stati membri assicurano che gli abbonati abbiano la possibilità di decidere se i loro dati personali - e, nell'affermativa, quali - debbano essere riportati in un elenco pubblico, sempreché tali dati siano pertinenti per gli scopi dell'elenco dichiarati dal suo fornitore. Gli Stati membri provvedono affinché gli abbonati abbiano le possibilità di verificare, rettificare o ritirare tali dati. Il fatto che i dati non siano riportati in un elenco pubblico di abbonati la verifica, la correzione o il ritiro dei dati non devono comportare oneri.
3. Gli 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.
4. I paragrafi 1 e 2 si applicano agli abbonati che siano persone fisiche. Gli Stati membri assicurano inoltre, nel quadro del diritto comunitario e della normativa nazionale applicabile, un'adeguata tutela degli interessi legittimi degli abbonati che non siano persone fisiche relativamente all'inclusione negli elenchi pubblici.

## Comunicazioni indesiderate

1. L'uso di sistemi automatizzati di chiamata senza intervento di un operatore (dispositivi automatici di chiamata), del telefax o della posta elettronica (**inclusi SMS (Short Message Service) e MMS (Multi Media Service)**) a fini di commercializzazione diretta è consentito soltanto nei confronti degli abbonati **o degli utenti** che abbiano espresso preliminarmente il loro consenso.
  
2. Fatto salvo il paragrafo 1, allorché una persona fisica o giuridica ottiene dai suoi clienti le coordinate elettroniche per la posta elettronica nel contesto della vendita di un prodotto o servizio ai sensi della direttiva 95/46/CE, la medesima persona fisica o giuridica può utilizzare tali coordinate elettroniche a scopi di commercializzazione diretta di propri analoghi prodotti o servizi, a condizione che ai clienti sia offerta in modo chiaro e distinto **al momento della raccolta delle coordinate** [...] e ad ogni messaggio la possibilità di opporsi, gratuitamente e in maniera agevole, all'uso di tali coordinate elettroniche qualora il cliente non abbia rifiutato inizialmente tale uso.
  
3. Gli Stati membri adottano le misure appropriate per garantire che [...] le comunicazioni indesiderate a scopo di commercializzazione diretta, in casi diversi da quelli di cui ai paragrafi 1 e 2, non siano permesse se manca il consenso degli abbonati **o utenti** interessati oppure se gli abbonati **o utenti** esprimono il desiderio di non ricevere questo tipo di chiamate; la scelta tra queste due possibilità è effettuata dalla normativa nazionale, **tenendo conto del fatto che entrambe le possibilità devono essere gratuite per l'abbonato**.
  
4. In ogni caso, è vietata la prassi di inviare messaggi di posta elettronica a scopi di commercializzazione diretta camuffando o celando l'identità del mittente da parte del quale la comunicazione è effettuata, **o in violazione dell'articolo 6 della direttiva 2003/31/CE**, o senza fornire un indirizzo valido cui il destinatario possa inviare una richiesta di cessazione di tali comunicazioni.

5. I paragrafi 1 e 3 si applicano agli abbonati che siano persone fisiche. Gli Stati membri garantiscono inoltre, nel quadro del diritto comunitario e della normativa nazionale applicabile, un'adeguata tutela degli interessi legittimi degli abbonati che non siano persone fisiche relativamente alle comunicazioni indesiderate.

**6. Fatti salvi i ricorsi amministrativi che possono essere presentati, in particolare, a norma dell'articolo 15 bis, paragrafo 2, gli Stati membri garantiscono che ogni persona fisica o giuridica [...] che abbia subito effetti pregiudizievoli a seguito delle violazioni delle disposizioni nazionali adottate ai sensi del presente articolo e abbia pertanto un interesse legittimo alla cessazione o al divieto di tali violazioni, in particolare un fornitore di servizi di comunicazione elettronica che intenda tutelare i propri legittimi interessi commerciali [...], abbia il diritto di promuovere un'azione giudiziaria contro tali violazioni. Gli Stati membri possono inoltre stabilire regole specifiche relative alle sanzioni applicabili ai fornitori di servizi di comunicazione elettronica che con la loro [...] negligenza contribuiscono alla violazione delle disposizioni nazionali adottate ai sensi del presente articolo.**

*(35) I fornitori di servizi di comunicazione elettronica devono investire pesantemente nella lotta contro le comunicazioni commerciali indesiderate ("spam"). A differenza degli utenti finali, essi possiedono le conoscenze e le risorse necessarie per individuare ed identificare coloro che inviano tali comunicazioni commerciali indesiderate. È necessario, pertanto, che i fornitori di servizi di posta elettronica e gli altri fornitori di servizi abbiano la possibilità di promuovere azioni giudiziarie contro i mittenti di comunicazioni commerciali indesiderate (spammer) **per tali violazioni** e di difendere quindi [...] gli interessi dei loro clienti [...] **quali parte integrante dei propri interessi commerciali legittimi.***

## *Articolo 14*

### **Caratteristiche tecniche e normalizzazione**

- 1 Salvo quanto disposto nei paragrafi 2 e 3, nell'attuare le disposizioni della presente direttiva gli Stati membri assicurano che non siano imposti, per i terminali o altre apparecchiature di comunicazione elettronica, norme inderogabili relative a caratteristiche tecniche specifiche che possano ostacolare l'immissione sul mercato e la libera circolazione di tali apparecchiature tra i vari Stati membri e al loro interno.
  
2. Qualora talune disposizioni della presente direttiva possano essere attuate soltanto attraverso la prescrizione di caratteristiche tecniche specifiche per le reti di comunicazione elettronica, gli Stati membri informano la Commissione secondo le procedure di cui alla direttiva 98/34/CE del Parlamento europeo e del Consiglio, del 22 giugno 1998, che prevede una procedura di informazione nel settore delle norme e delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione(9).
  
3. All'occorrenza, possono essere adottate misure dirette a garantire che le apparecchiature terminali siano costruite in maniera compatibile con il diritto degli utenti di tutelare e controllare l'uso dei loro dati personali in conformità della direttiva 1999/5/CE e della decisione 87/95/CEE del Consiglio, del 22 dicembre 1986, relativa alla normalizzazione nel settore delle tecnologie dell'informazione delle telecomunicazioni(10).

### *Articolo 14 bis*

**Comitato**

**Soppresso**

**Applicazione di alcune disposizioni della direttiva 95/46/CE**

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

1bis. Il paragrafo 1 non si applica ai dati la cui conservazione è specificamente prevista dalla direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione, ai fini di cui all'articolo 1, paragrafo 1, di tale direttiva.

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

3. Il gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito dall'articolo 29 della direttiva 95/46/CE, svolge i compiti di cui all'articolo 30 della direttiva stessa anche per quanto concerne materie disciplinate dalla presente direttiva, segnatamente la tutela dei diritti e delle libertà fondamentali e degli interessi legittimi nel settore delle comunicazioni elettroniche.

## **Articolo 15 bis**

### **Attuazione e controllo**

- 1. Gli Stati membri determinano le sanzioni da irrogare in caso di violazione delle norme nazionali di attuazione della presente direttiva e prendono tutti i provvedimenti necessari per la loro applicazione. Le sanzioni previste devono essere effettive, proporzionate e dissuasive e possono essere applicate per coprire la durata della violazione, anche se a tale violazione è stato successivamente posto rimedio. Gli Stati membri notificano tali disposizioni alla Commissione entro e non oltre il termine per l'attuazione dell'atto modificativo e comunicano senza indugio, alla Commissione, ogni successiva modifica a queste disposizioni.**
  
- 2. [...] Gli Stati membri provvedono affinché [...] l'autorità nazionale competente e, se del caso, altri organismi nazionali, abbiano la competenza di ordinare la cessazione delle violazioni di cui al paragrafo 1.**
  
- 3. Gli Stati membri provvedono affinché le autorità nazionali [...] competenti e, se del caso, altri organismi nazionali, dispongano di tutte le risorse e di tutte le competenze necessarie, compresa la possibilità di ottenere ogni informazione pertinente di cui possano avere bisogno per applicare e controllare le disposizioni nazionali adottate conformemente alla presente direttiva.**
  
- 4. Per assicurare un'efficace collaborazione transfrontaliera nell'applicazione delle norme nazionali adottate conformemente alla presente direttiva e per creare condizioni armonizzate per la fornitura di servizi che comportino flussi di dati transfrontalieri, la Commissione può adottare raccomandazioni dopo aver consultato [...] l'ENISA, il Gruppo dell'articolo 29 e le autorità di regolamentazione pertinenti.**

[...]

(36) *La necessità di garantire un livello adeguato di protezione della vita privata e dei dati personali trasmessi e trattati attraverso l'uso delle reti di comunicazione elettronica nella Comunità implica il conferimento di competenze effettive di applicazione e controllo, tali da costituire un valido incentivo all'osservanza delle norme. È opportuno che le autorità nazionali [...]competenti e, se del caso, altri organismi nazionali siano dotati delle competenze e delle risorse sufficienti per poter indagare efficacemente sui casi di inosservanza delle norme e, in particolare, che abbiano la possibilità di ottenere tutte le informazioni pertinenti di cui potrebbero avere bisogno per dare seguito alle denunce ed imporre sanzioni se necessario.*

(36 bis) *L'attuazione e il controllo delle disposizioni della presente direttiva richiedono spesso la cooperazione tra autorità nazionali di regolamentazione di due o più Stati membri, ad esempio nella lotta contro spam e software spia transfrontalieri. Al fine di assicurare una buona e rapida cooperazione in tali casi, nelle raccomandazioni dovrebbero essere definite procedure relative ad esempio alla quantità e al formato delle informazioni scambiate tra autorità o alle scadenze. Tali procedure consentiranno anche di armonizzare gli obblighi che ne risulteranno per gli operatori del mercato, contribuendo alla creazione di condizioni di parità nella Comunità.*

#### Articolo 16

#### Disposizioni transitorie

1. L'articolo 12 non si applica agli elenchi già prodotti o immessi sul mercato su supporto cartaceo o elettronico off-line prima dell'entrata in vigore delle disposizioni nazionali adottate in forza della presente direttiva.

2. Se i dati personali degli abbonati a servizi pubblici fissi o mobili di telefonia vocale sono stati inseriti in un elenco pubblico degli abbonati in conformità con le disposizioni della direttiva 95/46/CE e dell'articolo 11 della direttiva 97/66/CE prima dell'entrata in vigore delle disposizioni nazionali adottate conformemente alla presente direttiva, i dati personali di tali abbonati possono restare inseriti in tale elenco pubblico cartaceo o elettronico, comprese le versioni con funzioni di ricerca inverse, salvo altrimenti da essi comunicato dopo essere stati pienamente informati degli scopi e delle possibilità in conformità con l'articolo 12 della presente direttiva.

*[Articolo 4  
Attuazione*

*Articolo 5  
Entrata in vigore*

*Articolo 6  
Destinatari]*

---