I

(Risoluzioni, raccomandazioni e pareri)

PARERI

GARANTE EUROPEO DELLA PROTEZIONE DEI DATI

Parere del garante europeo della protezione dei dati sulla proposta di direttiva del Parlamento europeo e del Consiglio recante modifica, tra l'altro, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)

(2008/C 181/01)

IL GARANTE EUROPEO DELLA PROTEZIONE DEI DATI,

visto il trattato che istituisce la Comunità europea, in particolare l'articolo 286,

vista la Carta dei diritti fondamentali dell'Unione europea, in particolare l'articolo 8,

vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati ([1]),

vista la direttiva 2002/58 del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche ([2]),

visto il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati, in particolare l'articolo 41 ([3]),

vista la richiesta di parere a norma dell'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001, ricevuta il 16 novembre 2007 dalla Commissione europea,

HA ADOTTATO IL SEGUENTE PARERE:

I. **INTRODUZIONE**

1. Il 13 novembre 2007 la Commissione ha adottato una proposta di direttiva recante modifica, tra l'altro, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (in appresso «la proposta» o «le modifiche proposte»). Solitamente, e anche nel presente parere, si fa riferimento alla versione attuale della direttiva 2002/58/CE come alla direttiva relativa alla vita privata e alle comunicazioni elettroniche.

([1]) GU L 281 del 23.11.1995, pag. 31.
([2]) GU L 201 del 31.7.2002, pag. 37.
([3]) GU L 8 del 12.1.2001, pag. 1.

2. La proposta mira a rafforzare la tutela della vita privata e dei dati personali nel settore delle comunicazioni elettroniche. Ciò è ottenuto non trasformando interamente la direttiva vigente relativa alla vita privata e alle comunicazioni elettroniche, ma piuttosto proponendo modifiche ad hoc di detta direttiva, principalmente nell'intento di rafforzare le disposizioni in materia di sicurezza e di migliorare i meccanismi di controllo dell'attuazione.

3. La proposta è parte di una riforma più ampia delle cinque direttive UE sulle telecomunicazioni («pacchetto telecomunicazioni»). Oltre alle proposte di riesame del pacchetto telecomunicazioni ([1]) la Commissione ha altresì contemporaneamente adottato una proposta di regolamento che istituisce un'Autorità europea del mercato delle comunicazioni elettroniche ([2]).

4. Le osservazioni contenute nel presente parere sono limitate alle modifiche proposte per la direttiva relativa alla vita privata e alle comunicazioni elettroniche, a meno che tali modifiche si basino su concetti o disposizioni contenute nelle proposte di riesame del pacchetto telecomunicazioni. Inoltre talune osservazioni contenute nel presente parere si riferiscono a disposizioni della direttiva relativa alla vita privata e alle comunicazioni elettroniche che non sono state modificate dalla proposta.

5. Il presente parere tratta le questioni seguenti: i) campo di applicazione della direttiva relativa alla vita privata e alle comunicazioni elettroniche, in particolare, dei servizi interessati (proposta di modifica dell'articolo 3, paragrafo 1); ii) notifica delle violazioni di sicurezza (proposta di aggiunta dei paragrafi 3 e 4 all'articolo 4); iii) disposizioni su marcatori («cookie»), software spia e dispositivi simili (proposta di modifica dell'articolo 5, paragrafo 3); iv) ricorsi promossi dai fornitori dei servizi di comunicazione elettronica e da altre persone giuridiche (proposta di aggiunta del paragrafo 6 all'articolo 13) e v) rafforzamento delle disposizioni in materia di controllo dell'attuazione (proposta di aggiunta dell'articolo 15 *bis*).

Consultazioni con il GEPD e consultazioni pubbliche allargate

6. La proposta è stata inviata dalla Commissione al GEPD il 16 novembre 2007. Il GEPD interpreta questa comunicazione come una richiesta di parere per le istituzioni e gli organismi comunitari, come previsto all'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001 concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati [in appresso «il regolamento (CE) n. 45/2001»].

7. Prima dell'adozione della proposta, la Commissione ha consultato in maniera informale il GEPD sul progetto di proposta; il GEPD se ne è compiaciuto poiché ha avuto così modo di formulare suggerimenti sul progetto di proposta prima dell'adozione da parte della Commissione. Constata con soddisfazione che taluni suoi suggerimenti sono riflessi nella proposta.

8. L'adozione della proposta è stata preceduta da una ampia consultazione pubblica, prassi apprezzata dal GEPD. Infatti, nel giugno 2006 la Commissione ha avviato una consultazione pubblica riguardo alla sua comunicazione sul riesame del pacchetto telecomunicazioni, in cui espone il suo punto di vista sulla situazione e prospetta alcune proposte di modifiche ([3]). Il Gruppo dell'articolo 29 per la tutela dei dati, di cui il GEPD è membro, ha usato questa opportunità per comunicare il suo punto di vista sulle modifiche proposte in un parere adottato il 26 settembre 2006 ([4]).

([1]) Le modifiche proposte alle direttive sulle telecomunicazioni sono avanzate nelle proposte seguenti: i) proposta di direttiva del Parlamento europeo e del Consiglio recante modifica delle direttive 2002/21/CE che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica, 2002/19/CE relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate, e all'interconnessione delle medesime e 2002/20/CE relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica, del 13 novembre 2007, COM(2007) 697 defin.; ii) 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, del 13 novembre 2007, COM(2007) 698 defin.

([2]) Proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un'Autorità europea del mercato delle comunicazioni elettroniche, del 13 novembre 2007, COM(2007) 699 defin.

([3]) Comunicazione sul quadro normativo comunitario per le reti ed i servizi di comunicazione elettronica [SEC(2006) 816] adottata il 29 giugno 2006. La comunicazione era completata da un documento di lavoro della Commissione [COM(206) 334 defin.].

([4]) Parere 8/2006 sulla revisione del quadro normativo per le comunicazioni ed i servizi di comunicazione elettronica, con particolare attenzione sulla direttiva relativa alla vita privata e alle comunicazioni elettroniche, adottato il 26 settembre 2006.

Parere globale del GEPD

9. Globalmente il parere del GEPD sulla proposta è positivo. Il GEPD sostiene pienamente gli obiettivi a cui mira la Commissione adottando una proposta che rafforza la tutela della vita privata e dei dati personali nel settore delle comunicazioni elettroniche. Il GEPD si compiace particolarmente dell'adozione di un sistema obbligatorio di notifica delle violazioni di sicurezza (modifica dell'articolo 4 della direttiva relativa alla vita privata e alle comunicazioni elettroniche, tramite l'aggiunta dei paragrafi 3 e 4). Quando si verificano violazioni dei dati, la notifica presenta vantaggi evidenti: rafforza l'attendibilità delle organizzazioni, incoraggia le imprese ad attuare severe misure di sicurezza e permette l'individuazione delle tecnologie più affidabili in materia di protezione delle informazioni. Inoltre dà alle persone vittime della violazione l'opportunità di prendere misure per proteggersi dall'usurpazione di identità o da altro abuso delle informazioni personali che le riguardano.

10. Il GEPD accoglie con favore altre modifiche della proposta, ad esempio la capacità delle persone giuridiche con interessi legittimi di ricorrere contro quelli che violano talune disposizioni della direttiva relativa alla vita privata e alle comunicazioni elettroniche (modifica dell'articolo 13, tramite l'aggiunta del paragrafo 6). Altresì positivo è il rafforzamento dei poteri di indagine delle autorità nazionali di regolamentazione, poiché permetterà loro di valutare se il trattamento dei dati è effettuato nel rispetto della legge e di individuare gli autori della violazione (aggiunta dell'articolo 15 *bis*, paragrafo 3). La possibilità di porre fine quanto prima al trattamento illecito dei dati personali e alle violazioni della vita privata è una misura necessaria per tutelare i diritti e le libertà delle persone. A tal fine è accolta con grande favore la proposta dell'articolo 15 *bis*, paragrafo 2, con cui si riconosce la facoltà delle autorità nazionali di regolamentazione di disporre la cessazione delle violazioni, permettendo loro di porre un termine immediato ai trattamenti che infrangono gravemente la legislazione.

11. L'approccio della proposta e la maggior parte delle modifiche proposte sono in linea con il punto di vista sulla futura politica in materia di protezione dei dati espresso nei precedenti pareri del GEPD ad esempio il parere sull'applicazione della direttiva sulla protezione dei dati ([1]). Tra l'altro, l'approccio si basa sulla convinzione che, sebbene non siano necessari nuovi principi di protezione dei dati, vi sia l'esigenza di norme più specifiche per trattare le questioni relative alla protezione dei dati sollevate dalle nuove tecnologie, ad esempio Internet, RFID, ecc. Vi è pure l'esigenza di strumenti che contribuiscano a far attuare e rendere efficace la legislazione sulla protezione dei dati, consentendo per esempio alle persone giuridiche di ricorrere contro violazioni della protezione dei dati e imponendo di notificare le violazioni di sicurezza ai responsabili del trattamento.

12. Nonostante l'approccio globalmente positivo della proposta, il GEPD si rammarica che la proposta non sia ambiziosa come avrebbe potuto. In effetti, a partire dal 2003 l'applicazione delle disposizioni contenute nella direttiva relativa alla vita privata e alle comunicazioni elettroniche, nonché l'analisi accurata del tema hanno mostrato che talune disposizioni sono tutt'altro che chiare e generano incertezza del diritto e problemi di conformità. È il caso, ad esempio, dei fornitori semipubblici di servizi di comunicazione elettronica per i quali non è chiaro in che misura rientrino nel campo di applicazione della direttiva relativa alla vita privata e alle comunicazioni elettroniche. Ci si sarebbe aspettato che la Commissione si servisse del riesame del pacchetto telecomunicazioni, in particolare della direttiva relativa alla vita privata e alle comunicazioni elettroniche, per risolvere alcuni dei problemi in sospeso. Inoltre nel trattare nuove questioni, come l'istituzione di un sistema obbligatorio di notifica delle violazioni, la proposta offre soltanto una soluzione parziale, non includendo tra le organizzazioni obbligate a notificare le violazioni di sicurezza, soggetti che trattano categorie di dati molto sensibili, per esempio le banche in linea o i fornitori di servizi sanitari in linea. Il GEPD si rammarica per questo approccio.

13. Il GEPD auspica che durante l'iter legislativo della proposta, il legislatore tenga conto delle osservazioni e delle proposte contenute nel presente parere al fine di risolvere le questioni che la proposta della Commissione non è riuscita ad affrontare.

([1]) Parere del garante europeo della protezione dei dati, del 25 luglio 2007, sulla comunicazione della Commissione al Parlamento europeo e al Consiglio sul seguito dato al programma di lavoro per una migliore applicazione della direttiva sulla protezione dei dati (GU C 255 del 27.10.2007, pag. 1).

II. ANALISI DELLA PROPOSTA

II.1. Campo di applicazione della direttiva relativa alla vita privata e alle comunicazioni elettroniche, in particolare, dei servizi interessati

14. Un punto chiave nell'attuale direttiva relativa alla vita privata e alle comunicazioni elettroniche è il campo di applicazione. La proposta contiene taluni elementi positivi che permetterebbero di definire e chiarire il campo di applicazione della direttiva, in particolare riguardo ai servizi interessati, e che sono discussi in appresso al punto i). Sfortunatamente le modifiche proposte non risolvono tutti i problemi sul tappeto. Come discusso al punto ii) in appresso, le modifiche non cercano purtroppo di ampliare il campo di applicazione della direttiva per includervi i servizi di comunicazione elettronica sulle reti private.

15. L'articolo 3 della direttiva relativa alla vita privata e alle comunicazioni elettroniche descrive i servizi coperti dalla direttiva stessa, in altre parole, i servizi a cui si applicano gli obblighi in essa enunciati: «La presente direttiva si applica al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione».

16. Pertanto i servizi coperti dalla direttiva relativa alla vita privata e alle comunicazioni elettroniche sono i fornitori di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche («PPECS»). La definizione di PPECS figura all'articolo 2, lettera c), della direttiva quadro ([1]). Le reti pubbliche di comunicazione sono definite all'articolo 2, lettera d), della stessa direttiva quadro ([2]). Esempi di attività dei PPECS sono: la fornitura di accesso a Internet, la trasmissione di informazioni attraverso reti elettroniche, le connessioni telefoniche fisse e mobili, ecc.

i) *Modifica proposta per l'articolo 3 della direttiva relativa alla vita privata e alle comunicazioni elettroniche: i servizi interessati devono includere le reti di comunicazione pubbliche che supportano i dispositivi di raccolta e di identificazione dei dati*

17. La proposta modifica l'articolo 3 della direttiva relativa alla vita privata e alle comunicazioni elettroniche, specificando che le reti pubbliche di comunicazione elettronica includono «reti di comunicazione pubbliche che supportano i dispositivi di raccolta e di identificazione dei dati». Il considerando 28 spiega che lo sviluppo di applicazioni che comportano la raccolta di informazioni, inclusi i dati personali, e che utilizzano le radiofrequenze, come l'RFID, deve essere soggetto alla direttiva relativa alla vita privata e alle comunicazioni elettroniche, quando dette applicazioni sono collegate a reti o usano servizi di comunicazione elettronica.

18. Il GEPD giudica positivamente questa disposizione poiché essa chiarisce che una serie di applicazioni RFID rientrano nel campo di applicazione della direttiva relativa alla vita privata e alle comunicazioni elettroniche, fugando così parte dell'incertezza su questo punto ed eliminando definitivamente fraintendimenti o interpretazioni errate della legislazione.

19. In effetti, ai sensi dell'articolo 3 della vigente direttiva relativa alla vita privata e alle comunicazioni elettroniche, talune applicazioni RFID sono già coperte dalla direttiva. Questo accade per un insieme di ragioni. In primo luogo perché le applicazioni RFID rientrano nella definizione di servizi di comunicazione elettronica. In secondo luogo perché sono fornite su una rete di comunicazione elettronica in quanto supportate da un sistema di trasmissione dei segnali senza cavo. Infine la rete può essere

([1]) Direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (GU L 108 del 24.4.2002, pag. 33). La direttiva quadro delimita ciò che si intende per servizio di comunicazione elettronica, segnatamente: i) un «servizio di comunicazione elettronica» è un servizio fornito di norma a pagamento, consiste nella trasmissione di segnali su reti e comprende servizi di telecomunicazioni e di trasmissione nelle reti; ii) i servizi che forniscono contenuti trasmessi utilizzando reti e servizi di comunicazione elettronica sono esclusi dalla definizione di servizi di comunicazione elettronica; iii) fornitura di servizi significa: realizzazione, gestione, controllo o messa a disposizione di una rete; iv) i servizi di comunicazione elettronica non includono i servizi della società dell'informazione, che sono definiti nella direttiva sul commercio elettronico come servizio/i, prestato/i normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi.

([2]) Per rete pubblica di comunicazioni si intende: una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazioni elettroniche accessibili al pubblico.

pubblica e privata. Se pubblica, le applicazioni RFID saranno considerate «servizi interessati» rientrando così nel campo di applicazione della direttiva relativa alla vita privata e alle comunicazioni elettroniche. Tuttavia la modifica proposta eliminerà qualsiasi dubbio restante in merito a tale questione, migliorando così la certezza del diritto.

20. Naturalmente, come sottolineato nel precedente parere del GEPD sull'RFID ([1]), questa disposizione non esclude che possa essere necessario adottare strumenti giuridici supplementari per quanto riguarda l'RFID. Tuttavia tali misure dovrebbero essere adottate in un altro contesto, non nel quadro della proposta in esame.

ii) *Necessità di includere i servizi di comunicazione elettronica nelle reti private o semiprivate*

21. Il GEPD accoglie con favore i chiarimenti ora illustrati; si rammarica tuttavia che la proposta non abbia affrontato la questione della distinzione sempre meno netta tra reti pubbliche e private. Si rammarica altresì per il fatto che la definizione di servizi coperti dalla direttiva relativa alla vita privata e alle comunicazioni elettroniche non sia stata ampliata per includere le reti private. Nella sua attuale formulazione, l'articolo 3, paragrafo 1, della direttiva relativa alla vita privata e alle comunicazioni elettroniche si applica soltanto ai *servizi di comunicazione elettronica nelle reti pubbliche*.

22. Il GEPD rileva la tendenza dei servizi a divenire sempre più un mix di pubblico e privato. Basti pensare alle università che permettono a migliaia di studenti di usare Internet e la posta elettronica. La capacità di queste reti semipubbliche (o semiprivate) di incidere sulla vita privata è ovvia e pertanto giustifica che questo tipo di servizi debba essere soggetto alla stessa serie di norme che si applicano alle reti interamente pubbliche. Inoltre le reti private, come quelle dei datori di lavoro che forniscono agli impiegati un accesso Internet, dei proprietari di alberghi o residence che forniscono agli ospiti telefono e posta elettronica nonché degli Internet café, hanno un impatto sulla protezione dei dati e della vita privata degli utenti; se ne deduce che anch'essi dovrebbero rientrare nel campo di applicazione della direttiva relativa alla vita privata e alle comunicazioni elettroniche.

23. Infatti, la giurisprudenza di taluni Stati membri ha già stabilito che i servizi di comunicazione elettronica sulle reti private siano soggetti agli stessi obblighi previsti per quelle pubbliche ([2]). Anche in Germania, ai sensi della legislazione nazionale, le autorità incaricate della protezione dei dati hanno riscontrato che un'impresa potrebbe essere considerata un operatore di servizi pubblici di telecomunicazioni, qualora permetta l'uso privato della posta elettronica al suo interno e rientrando così nelle disposizioni della direttiva relativa alla vita privata e alle comunicazioni elettroniche.

24. In breve, la crescente importanza delle reti miste (privata/pubblica) e private nella vita di ogni giorno, insieme all'aumento del rischio per i dati personali e la vita privata, giustificano la necessità di applicare a tali servizi la stessa serie di norme che si applicano ai servizi pubblici di comunicazione elettronica. A tal fine il GEPD ritiene che la direttiva debba essere modificata per ampliare il suo campo di applicazione al fine di includere tale tipo di servizi privati; punto di vista condiviso dal Gruppo dell'«articolo 29» ([3]).

II.2. **Notifica delle violazioni di sicurezza: modifica dell'articolo 4**

25. L'articolo 4 della direttiva relativa alla vita privata e alle comunicazioni elettroniche è modificato con l'aggiunta di due nuovi paragrafi (3 e 4) che istituiscono l'obbligo di notifica delle violazioni di sicurezza. In effetti, ai sensi dell'articolo 4, paragrafo 3, i PPECS sono obbligati, da una parte, a notificare alle autorità nazionali di regolamentazione, senza indugio, la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la rivelazione, o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di servizi di comunicazione elettronica (nell'insieme un «danneggiamento dei dati»); dall'altra, sono anche obbligati a notificare ai loro clienti.

([1]) Parere del 20 dicembre 2007 sulla comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni: L'identificazione a radiofrequenza (RFID) in Europa: verso un quadro politico documento COM(2007) 96.

([2]) Per esempio la sentenza della Corte d'appello di Parigi nella causa BNP Parisbas contro World Press Online, del 4 febbraio 2005, ha concluso che non c'era distinzione tra i fornitori di servizi Internet che offrivano un accesso a Internet su base commerciale e i datori di lavoro che davano un accesso a Internet al proprio personale.

([3]) Parere 8/2006 sulla revisione del quadro normativo per le comunicazioni ed i servizi di comunicazione elettronica, con particolare attenzione sulla direttiva relativa alla vita privata e alle comunicazioni elettroniche, adottato il 26 settembre 2006.

Vantaggi di questo obbligo

26. Il GEPD accoglie con favore queste disposizioni (articolo 4, paragrafi 3 e 4) che introducono una notifica obbligatoria delle violazioni di sicurezza. Questa comporta effetti positivi dal punto di vista della protezione dei dati personali e della vita privata, già stati dimostrati negli Stati Uniti, paese in cui la legislazione a livello statale in materia di notifica delle violazioni è in vigore da vari anni.

27. In primo luogo la legislazione in materia di notifica delle violazioni aumenta l'affidabilità dei PPECS riguardo alle informazioni che sono state compromesse. Nel quadro della politica in materia di protezione dei dati o della vita privata, l'attendibilità significa che ciascuna organizzazione è responsabile delle informazioni che le sono state affidate e che sono sotto il suo controllo. Imporre l'obbligo di notifica equivale a riaffermare che da una parte, i dati danneggiati erano sotto il controllo dei PPECS e, dall'altra, che incombe a queste organizzazioni la responsabilità delle misure necessarie relativamente a tali dati.

28. In secondo luogo l'esistenza di una notifica della violazione di sicurezza si è dimostrata un fattore trainante per gli investimenti nella sicurezza da parte delle organizzazioni che trattano i dati personali. Infatti, il semplice fatto di dover notificare pubblicamente le violazioni di sicurezza porta le organizzazioni ad attuare norme di sicurezza più severe che tutelano le informazioni personali e prevengono le violazioni. Inoltre la notifica delle violazioni di sicurezza aiuterà ad individuare le soluzioni e i meccanismi più efficaci in materia di sicurezza, e a realizzare analisi statistiche affidabili al riguardo. Per un lungo periodo c'è stata carenza di dati precisi sulle disfunzioni della sicurezza delle informazioni e sulle tecnologie più opportune per proteggere le informazioni. È probabile che questo problema venga risolto con gli obblighi di notifica delle violazioni di sicurezza, come è avvenuto negli Stati Uniti grazie alla legislazione sulla comunicazione delle violazioni, perché la notifica informerà sulle tecnologie più esposte alle violazioni ([1]).

29. Infine la notifica delle violazioni di sicurezza informa le persone sui rischi che corrono allorché i loro dati personali sono danneggiati e le aiuta a prendere le misure necessarie per ridurre tali rischi. Ad esempio in caso di danneggiamento delle coordinate bancarie la persona che ne è informata può decidere di modificare gli estremi per l'accesso al suo conto bancario al fine di impedire che qualcuno si impadronisca di queste informazioni e le usi per scopi illeciti (atto noto come «usurpazione d'identità») In sintesi questo obbligo limita la possibilità di subire un'usurpazione d'identità e può inoltre assistere le vittime nelle azioni necessarie a risolvere tali problemi.

Carenze della modifica proposta

30. Il GEPD, benché si compiaccia del sistema di notifica delle violazioni di sicurezza di cui all'articolo 4, paragrafi 3 e 4, ne avrebbe preferito un'applicazione su scala più vasta in modo da includere i fornitori di servizi della società dell'informazione. La normativa contemplerebbe così, tra gli altri, le banche in linea, le imprese in linea e i fornitori di servizi sanitari in linea ([2]).

31. I motivi che giustificano l'obbligo di notifica delle violazioni di sicurezza per i fornitori dei servizi di comunicazione elettronica accessibili al pubblico, ossia i PPECS, sono altresì validi per altre organizzazioni che pure trattano volumi massicci di dati personali la cui diffusione sarebbe particolarmente dannosa per gli interessati. Vi sono tra queste le banche in linea, gli intermediari che forniscono dati e altri fornitori di servizi in linea, ad esempio quelli che trattano dati sensibili (tra i quali i dati sanitari, le opinioni politiche, ecc.). Se le informazioni detenute da banche o imprese in linea, che possono comprendere non soltanto numeri di conti bancari ma anche estremi di carte di credito, sono compromesse, si possono verificare usurpazioni di identità, nel qual caso è fondamentale che le persone interessate siano informate per prendere le misure necessarie. Relativamente ai servizi sanitari in linea anche se le persone interessate non subiscono danni di natura finanziaria, subiranno in tutta probabilità danni di altra natura qualora siano compromesse informazioni sensibili.

([1]) Cfr. la relazione «Security Economics and the Internal Market», commissionata dall'Agenzia europea per la sicurezza delle reti e dell'informazione ai proff. Ross Anderson, Rainer Böhme, Richard Clayton e Tyler Moore. La relazione è disponibile sul sito:
http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf

([2]) I fornitori di servizi della società dell'informazione sono definiti nella direttiva sul commercio elettronico come servizio/i, prestato/i normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi.

32. Inoltre, estendendo la portata dell'obbligo, i benefici sopradescritti, che dovrebbero derivare dall'imposizione di tale obbligo, non saranno limitati a un settore di attività, ossia quella dei fornitori di servizi di comunicazione elettronica accessibili al pubblico, ma saranno estesi ai servizi della società dell'informazione in generale. Infatti, l'obbligo di notifica delle violazioni di sicurezza imposto ai servizi della società dell'informazione, ad esempio le banche in linea, non solo accrescerà la loro responsabilità ma li motiverà a rafforzare le loro misure di sicurezza e a eliminare in tal modo in futuro il rischio di violazioni di sicurezza.

33. L'applicazione ad altri soggetti, diversi dai PPECS, ha dei precedenti nella direttiva relativa alla vita privata e alle comunicazioni elettroniche, ad esempio nell'articolo 5 sulla riservatezza delle comunicazioni e nell'articolo 13 sulle comunicazioni indesiderate (spam). Ciò conferma che, in passato, il legislatore aveva deciso assai saggiamente di estendere il campo di applicazione di talune disposizioni della direttiva in questione poiché lo riteneva opportuno e necessario. Il GEPD auspica che il legislatore non esiterà ora a seguire un approccio analogo, flessibile e sensato, estendendo il campo di applicazione dell'articolo 4 per comprendervi i fornitori di servizi della società dell'informazione. A tal fine sarebbe sufficiente un riferimento nell'articolo 4, paragrafo 3, ai fornitori di servizi della società dell'informazione, così formulato: «Se si produce una violazione di sicurezza che comporta accidentalmente o (…), il fornitore dei servizi di comunicazione elettronica accessibili al pubblico e il fornitore di servizi della società dell'informazione comunicano (…) l'avvenuta violazione all'abbonato e all'autorità nazionale di regolamentazione».

34. Secondo il GEPD questo obbligo e la relativa imposizione sia ai PPECS sia ai fornitori di servizi della società dell'informazione sarebbero la prima tappa di uno sviluppo che, a termine, potrà applicarsi a tutti i responsabili del trattamento in generale.

Quadro giuridico specifico per le violazioni di sicurezza, da trattare attraverso la procedura di comitato

35. La proposta non tratta una serie di questioni connesse con l'obbligo di notifica delle violazioni di sicurezza Tra le questioni che occorre trattare, vi sono le circostanze della notifica, il formato e le procedure applicabili. Per contro l'articolo 4, paragrafo 4, della proposta prevede che queste decisioni siano adottate con una procedura di comitato ([1]), segnatamente il comitato per le comunicazioni istituito dall'articolo 22 della direttiva quadro, ai sensi della decisione del Consiglio, del 28 giugno 1999. In particolare tali misure sarebbero adottate a norma dell'articolo 5 della decisione del Consiglio, del 28 giugno 1999, che stabilisce le regole della procedura di regolamentazione per quanto riguarda «le misure di portata generale intese ad applicare le disposizioni essenziali di atti di base».

36. Il GEPD non è contrario a demandare tali questioni alla legislazione di attuazione. L'adozione della legislazione mediante procedura di comitato può abbreviare l'iter legislativo. La procedura di comitato contribuirà inoltre ad assicurare l'armonizzazione, il che è senz'altro un obiettivo da raggiungere.

37. Tenuto conto del numero elevato di questioni da trattare nelle misure di attuazione e della loro rilevanza, come di seguito evidenziato, sembra opportuno affrontarle insieme in un unico atto legislativo piuttosto che secondo un approccio frammentario, in cui alcune sarebbero trattate nella direttiva relativa alla vita privata e alle comunicazioni elettroniche e altre lasciate alla legislazione di attuazione. Pertanto va accolto con favore l'approccio della Commissione, che consiste nel demandare queste decisioni alla legislazione di attuazione, da adottarsi previa consultazione del GEPD e come è auspicabile di altre parti interessate (v. infra).

Questioni da trattare nelle misure di attuazione

38. Se le questioni da trattare nelle misure di attuazione si possono prevedere con un certo grado di dettaglio, l'importanza di queste misure emergerà con chiarezza. Infatti, le misure di attuazione potranno stabilire le norme per le notifiche. Ad esempio specificheranno in cosa consiste una violazione di sicurezza, nonché le condizioni e i termini per notificarla alle persone interessate e alle autorità.

([1]) Procedure legislative CE in cui ci si avvale di comitati composti di rappresentanti dei governi degli Stati membri a livello di funzionari pubblici.

39. Secondo il GEPD la direttiva relativa alla vita privata e alle comunicazioni elettroniche, in particolare l'articolo 4, non dovrebbe contenere alcuna eccezione all'obbligo di notifica. A questo riguardo il GEPD è favorevole all'approccio della Commissione, concretato nell'articolo 4, che stabilisce l'obbligo di notifica senza alcuna eccezione ma consente di trattare tale ed altre questioni nelle misure di attuazione. Pur consapevole delle argomentazioni che potrebbero giustificare alcune eccezioni all'obbligo, il GEPD è favorevole a che tale e altre questioni siano attentamente trattate nella legislazione di attuazione, dopo una discussione approfondita e omnicomprensiva di tutte le questioni sul tappeto. Come detto la complessità delle questioni connesse con l'obbligo di notificare le violazioni di sicurezza, opportunità di eventuali eccezioni o limitazioni compresa, richiede un trattamento unificato, vale a dire con un unico atto legislativo esclusivamente dedicato a tali questioni.

Consultazioni con il GEPD ed esigenza di consultazioni allargate

40. Le misure di attuazione incideranno notevolmente sulla protezione dei dati personali: è quindi importante che prima di adottarle la Commissione conduca le opportune consultazioni. Per questo motivo il GEPD accoglie con favore l'articolo 4, paragrafo 4, della proposta in cui si stabilisce espressamente che, prima di adottare le misure di attuazione, la Commissione consulterà il Garante europeo della protezione dei dati. Tali misure non solo riguarderanno la protezione dei dati personali e della vita privata delle persone ma avranno anche un forte impatto su di essa. È dunque importante ottenere il parere del GEPD come richiesto dall'articolo 41 del regolamento (CE) n. 45/2001.

41. Oltre alla consultazione del GEPD può essere opportuno prevedere una disposizione che stabilisca che il progetto di misure di attuazione sia sottoposto a consultazione pubblica, per raccogliere pareri e promuovere la condivisione delle esperienze di migliori pratiche in questa materia. Si aprirebbe in tal modo un idoneo canale che permetterebbe non solo all'industria ma anche ad altri soggetti interessati, tra cui altre autorità incaricate della protezione dei dati e il Gruppo dell'articolo 29, di esprimere i loro pareri. L'esigenza di consultazione pubblica risulta ancor più pressante se si considera che la procedura di adozione della legislazione è quella di comitato, con un intervento limitato del Parlamento europeo.

42. Il GEPD rileva che l'articolo 4, paragrafo 4, della proposta prevede che la Commissione consulti anche l'Autorità europea del mercato delle comunicazioni elettroniche prima di adottare norme di attuazione. Al riguardo il GEPD apprezza il principio di consultare questa Autorità, depositaria dell'esperienza e conoscenze in materia di reti e sicurezza dell'informazione dell'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA). In attesa della creazione dell'Autorità europea del mercato delle comunicazioni elettroniche, può essere opportuno prevedere nella proposta di modifica (articolo 4, paragrafo 4), a titolo provvisorio, la consultazione dell'ENISA.

II.3. **Disposizioni sui marcatori («cookie»), software spia e dispositivi simili modifica dell'articolo 5, paragrafo 3**

43. L'articolo 5, paragrafo 3, della direttiva relativa alla vita privata e alle comunicazioni elettroniche tratta delle tecnologie che permettono l'accesso alle informazioni e l'archiviazione di informazioni nel terminale dell'utente, attraverso reti di comunicazione elettronica. Ad esempio l'articolo 5, paragrafo 3, si applica all'uso di cookie ([1]). Altri esempi sono l'uso di tecnologie quali i software spia (programmi di spionaggio nascosti) e i cavalli di Troia (programmi nascosti in messaggi o in altri software apparentemente innocui). Gli scopi di queste tecnologie variano enormemente e mentre alcune sono del tutto innocue o addirittura utili all'utente, altre sono molto pericolose e costituiscono una vera minaccia.

([1]) I cookie sono installati dai fornitori di servizi della società dell'informazione (ISSP — *Information Society Service Providers*) (fornitori di siti web) nei terminali degli utenti a scopi diversi, ad esempio riconoscere che si ricollega a un sito web. In pratica quando un sito web invia un cookie a un utente Internet un numero unico è assegnato al computer di questi (ossia il computer che ha ricevuto il cookie dal sito web A diventa il «computer che contiene il cookie 111»). Il sito web mantiene il numero come riferimento. Se l'utente del computer che ha ricevuto il cookie 111 non cancella il file corrispondente, alla visita successiva dello stesso sito web sarà da questo identificato come il computer che contiene il cookie 111. Il sito web deduce naturalmente che il computer ha già visitato il sito stesso. Il dispositivo che permette a un sito web di riconoscere un computer che si collega più volte è semplice. Quando il computer visitatore che contiene dei cookie, ad esempio il cookie 111, si collega di nuovo al sito visitato in precedenza e da cui è stato generato il cookie, cercherà nell'hard disk dell'utente il numero di file del cookie. Se il browser dell'utente trova un file cookie che corrisponde al numero di riferimento conservato dal sito web, informa il sito stesso che il computer contiene il cookie 111.

44. L'articolo 5, paragrafo 3, della direttiva relativa alla vita privata e alle comunicazioni elettroniche stabilisce le condizioni di accesso o archiviazione sul terminale degli utenti allorché si usano, tra l'altro, le tecnologie sopra descritte. In particolare in forza dell'articolo 5, paragrafo 3, i) gli utenti Internet devono essere informati in modo chiaro e completo, in conformità della direttiva 95/46/CE, tra l'altro sugli scopi del trattamento; e ii) devono poter rifiutare tale trattamento, ossia escludere il trattamento delle informazioni estratte dal proprio terminale.

Vantaggi della modifica proposta

45. Il campo di applicazione dell'attuale articolo 5, paragrafo 3, della direttiva relativa alla vita privata e alle comunicazioni elettroniche è limitato ai casi in cui l'accesso alle informazioni e l'archiviazione di informazioni nel terminale dell'utente sono effettuati tramite *reti di comunicazione elettronica*. Vi rientrano quindi i casi sopra descritti di uso dei cookie o di altre tecnologie, ad esempio i software spia, veicolati dalle reti di comunicazione elettronica. Tuttavia non è per nulla chiaro se l'articolo 5, paragrafo 3, si applica ai casi in cui tecnologie analoghe (cookie/software spia e simili) sono veicolate da software forniti su supporti esterni di memorizzazione e scaricate sul terminale dell'utente. La minaccia alla vita privata sussiste indipendentemente dal canale di comunicazione, la limitazione dell'articolo 5, paragrafo 3, ad un unico canale è pertanto inopportuna.

46. Il GEPD si compiace pertanto della modifica all'articolo 5, paragrafo 3, che, rimuovendo il riferimento alle «reti di comunicazione elettronica», di fatto amplia il campo di applicazione dell'articolo 5, paragrafo 3. In effetti, la versione modificata dell'articolo 5, paragrafo 3, comprende entrambe le situazioni in cui l'accesso alle informazioni e la loro archiviazione nel terminale degli utenti avvengono tramite reti di comunicazione elettronica ma anche tramite altri supporti esterni per l'archiviazione dei dati quali CD, CD-ROM, chiavi USB, ecc.

Archiviazione tecnica al fine di facilitare la trasmissione

47. L'ultima frase dell'articolo 5, paragrafo 3, della direttiva relativa alla vita privata e alle comunicazioni elettroniche rimane invariata nella versione modificata. Conformemente a questa frase i requisiti della prima frase dell'articolo 5, paragrafo 3, non vietano «l'eventuale archiviazione 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 (…)». Quindi le norme vincolanti della prima frase dell'articolo 5, paragrafo 3 (ossia la necessità di fornire informazioni e di offrire la possibilità di rifiutare), non si applicheranno quando l'accesso al terminale dell'utente o l'archiviazione di informazioni hanno il solo scopo di *facilitare* una trasmissione o quando sono strettamente necessari a fornire servizi della società dell'informazione richiesti dall'utente.

48. La direttiva non precisa quando l'accesso alle informazioni o la loro archiviazione hanno il solo scopo di facilitare una trasmissione o di fornire informazioni. Una situazione che sarebbe chiaramente coperta da questa eccezione è la creazione di una connessione a Internet. Infatti, per creare una connessione a Internet è necessario ottenere un indirizzo IP ([1]). Il fornitore dell'accesso a Internet chiederà al computer dell'utente finale talune informazioni che lo riguardano fornendogli in cambio un indirizzo IP. In questo caso le informazioni archiviate nel terminale dell'utente finale saranno trasferite al fornitore dell'accesso a Internet affinché tale accesso possa essere dato all'utente. In questo caso il fornitore dell'accesso a Internet è esentato sia dall'obbligo di dichiarare questa raccolta di informazioni, sia da quello di offrire il diritto di rifiutare, poiché ciò è necessario per poter fornire il servizio.

49. Una volta connesso a Internet, se un utente vuole collegarsi a un sito web, deve inviare una richiesta al server in cui è ospitato il sito stesso. Quest'ultimo risponderà se sa dove inviare le informazioni, cioè se conosce l'indirizzo IP dell'utente. A causa del tipo di archiviazione dell'indirizzo occorrerà nuovamente che il sito web a cui l'utente vuole collegarsi acceda alle informazioni archiviate sul terminale degli utenti Internet. Chiaramente anche questa transazione rientrerebbe nel campo di applicazione dell'eccezione. Di fatto sembra opportuno che questi casi non rientrino nel campo di applicazione dei requisiti dell'articolo 5, paragrafo 3.

([1]) Un indirizzo IP (indirizzo del protocollo Internet) è un indirizzo unico di cui si servono taluni dispositivi elettronici per identificarsi e comunicare reciprocamente su una rete che utilizza il protocollo Internet (IP) — più semplicemente, un indirizzo informatico. I dispositivi che partecipano alla rete — inclusi i router, i commutatori, i computer, i server di infrastruttura (ad es. NTP, DNS, DHCP, SNMP, ecc.), le stampanti, i fax Internet e taluni telefoni — possono avere il proprio indirizzo che è unico nell'ambito di una specifica rete. Alcuni indirizzi IP sono destinati ad essere unici nell'Internet globale, mentre altri devono essere unici soltanto nell'ambito di un'impresa.

50. Il GEPD ritiene opportuno esentare dalla necessità di informare e di dare la possibilità di rifiutare in situazioni come quelle illustrate sopra, quando l'archiviazione tecnica o l'accesso al terminale di un utente sono *necessari* al solo scopo di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica. Lo stesso dicasi quando l'archiviazione tecnica o l'accesso sono strettamente necessari al fine di fornire un servizio della società dell'informazione. Tuttavia il GEPD non vede la necessità di escludere dall'obbligo di fornire informazioni e di offrire il diritto di rifiutare nelle situazioni in cui l'archiviazione tecnica o l'accesso hanno il solo scopo di *facilitare* la trasmissione di una comunicazione. Ad esempio, conformemente all'ultima frase di questo articolo la persona interessata potrebbe non beneficiare del diritto ad essere informato del diritto di opporsi al trattamento dei suoi dati se un cookie raccogliesse i dati relativi alle sue preferenze linguistiche o al luogo in cui si trova (ad es. il Belgio, la Cina) in quanto questo tipo di cookie potrebbe essere presentato come se avesse l'obiettivo di facilitare la trasmissione di una comunicazione. Il GEPD è consapevole che, a livello di software, le persone interessate hanno in pratica la possibilità di rifiutare o modulare l'archiviazione di cookie. Tuttavia questa pratica non è appoggiata abbastanza chiaramente da alcuna disposizione giuridica che autorizzerebbe formalmente la persona interessata a difendere i suoi diritti nel contesto sopra descritto.

51. Per evitare questo inconveniente il GEPD propone di apportare una modifica di lieve entità all'ultima parte dell'articolo 5, paragrafo 3, che consiste nella soppressione del termine «facilitare» dalla frase: «non vieta l'eventuale archiviazione 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 (…)».

II.4. **Ricorsi dei PPECS delle persone giuridiche: aggiunta del paragrafo 6 all'articolo 13**

52. La proposta relativa all'articolo 13, paragrafo 6, introduce la possibilità di ricorsi civili per le persone fisiche o giuridiche con un interesse legittimo, in particolare i fornitori di servizi di comunicazione elettronica, che hanno l'interesse commerciale di opporsi alle violazioni dell'articolo 13 della direttiva relativa alla vita privata e alle comunicazioni elettroniche. Questo articolo tratta l'invio di comunicazioni commerciali indesiderate.

53. La modifica proposta permetterà, ad esempio, ai fornitori dell'accesso a Internet di lottare contro gli spammer che utilizzano abusivamente le loro reti, di citare in giudizio i soggetti che contraffanno gli indirizzi dei mittenti o che penetrano nei server per utilizzarli come relais delle spam, ecc.

54. La direttiva relativa alla vita privata e alle comunicazioni elettroniche non era chiara sul fatto di concedere ai PPECS il diritto di ricorso contro gli spammer e, in pochissime occasioni, i fornitori di servizi pubblici di comunicazione elettronica hanno intentato azioni contro la violazione dell'articolo 13 come attuato nella legislazione degli Stati membri ([1]). Riconoscendo ai fornitori di servizi di comunicazione elettronica il diritto di intentare ricorso per proteggere i loro interessi commerciali, la proposta conferma che la direttiva relativa alla vita privata e alle comunicazioni elettroniche intende non soltanto proteggere i singoli abbonati, ma anche i fornitori di servizi di comunicazione elettronica.

55. Il GEPD si compiace che la proposta introduca la possibilità per i fornitori di servizi di comunicazione elettronica di promuovere azioni giudiziarie contro coloro che inviano messaggi di posta elettronica indesiderata (spammer) per tutelare i propri interessi commerciali. Salvo casi eccezionali, i singoli abbonati non dispongono né dei mezzi finanziari, né degli incentivi per avviare questo tipo di azioni giudiziarie. Al contrario, i fornitori dell'accesso a Internet ed altri PPECS possiedono la solidità finanziaria e le capacità tecnologiche per indagare sulle campagne di spam ed individuarne gli autori, per cui è del tutto appropriato che abbiano il diritto di promuovere azioni giudiziarie contro gli spammer.

56. Il GEPD è particolarmente soddisfatto della modifica proposta in quanto essa consentirebbe anche alle associazioni di consumatori ed ai sindacati che rappresentano gli interessi dei consumatori vittime di spam di promuovere azioni giudiziarie per loro conto. Come affermato in precedenza, il danno inflitto ad una persona vittima di spam, considerato singolarmente, non è generalmente di entità tale da giustificare la promozione di azioni giudiziarie da parte della persona interessata. In realtà il GEPD aveva già proposto questa misura nel quadro generale delle violazioni della vita privata e della riservatezza dei

([1]) Un caso di ricorso è la causa Microsoft corporation contro Paul McDonald t/a Bizards UK [2006 All Er (D) 153].

dati nel suo parere sul seguito dato al programma di lavoro per una migliore applicazione della direttiva sulla protezione dei dati ([1]). Secondo l'opinione del GEPD, la proposta avrebbe potuto andare oltre e proporre azioni collettive, che autorizzano gruppi di cittadini a ricorrere congiuntamente all'azione legale in materie concernenti la protezione dei dati personali. Nel caso delle spam, qualora gli invii riguardino un numero elevato di persone, esiste la possibilità che gruppi di individui si associno ed avviino azioni collettive contro gli spammer.

57. Il GEPD si rammarica in particolare che la proposta limiti la possibilità per le persone giuridiche di promuovere azioni giudiziarie ai soli casi di violazione dell'articolo 13 della direttiva, ossia alle situazioni in cui si riscontra una violazione della disposizione relativa alle comunicazioni di posta elettronica indesiderate. In effetti, in base alla modifica proposta le persone giuridiche non potrebbero promuovere azioni giudiziarie riguardo a violazioni di altre disposizioni della direttiva relativa alla vita privata e alle comunicazioni elettroniche. Ad esempio, la disposizione attuale non consente ad una persona giuridica quale un'associazione di consumatori di promuovere azioni giudiziarie nei confronti di un fornitore dell'accesso a Internet che ha divulgato i dati personali di milioni di clienti. L'attuazione della direttiva relativa alla vita privata nel suo insieme, e non solo di un articolo specifico, sarebbe migliorata notevolmente se la disposizione di cui all'articolo 13, paragrafo 6, fosse generalizzata, in modo da consentire alle persone giuridiche di promuovere azioni giudiziarie in caso di violazione di qualsiasi disposizione della direttiva relativa alla vita privata e alle comunicazioni elettroniche.

58. Per risolvere tale problema il GEPD propone di trasferire il paragrafo 6 dell'articolo 13 in un articolo distinto (articolo 14). Inoltre, il testo dell'articolo 13, paragrafo 6, dovrebbe essere lievemente modificato come segue: invece di «ai sensi del presente articolo» si dovrebbe leggere «ai sensi della presente direttiva».

II.5. **Rafforzamento delle disposizioni di attuazione: aggiunta dell'articolo 15 *bis***

59. La direttiva relativa alla vita privata e alle comunicazioni elettroniche non contiene esplicite disposizioni di attuazione. Fa per contro riferimento alla sezione relativa all'attuazione della direttiva sulla protezione dei dati ([2]). Il GEPD si compiace del nuovo articolo 15 *bis* della proposta, che riguarda in modo esplicito gli aspetti relativi all'attuazione ai sensi della direttiva in questione.

60. In primo luogo, il GEPD prende atto che un'efficace politica di controllo dell'attuazione in questo settore presuppone, come proposto all'articolo 15 *bis*, paragrafo 3, che le autorità nazionali dispongono di poteri di indagine al fine di raccogliere le informazioni necessarie. Molto spesso le prove della violazione delle disposizioni della direttiva relativa alla vita privata e alle comunicazioni elettroniche saranno di natura elettronica e possono essere conservate in diversi computer, dispositivi o reti. In tale contesto è importante che agli organi preposti all'applicazione della legge sia data la possibilità di ottenere mandati di perquisizione che conferiscono poteri di ingresso, perquisizione e sequestro.

61. In secondo luogo, il GEPD si compiace in modo particolare della modifica proposta, ossia dell'articolo 15 *bis*, paragrafo 2, secondo cui le autorità nazionali di regolamentazione devono poter avviare azioni inibitorie, ossia ordinare la cessazione delle violazioni, nonché disporre dei poteri di indagine e delle risorse necessarie. Le autorità nazionali di regolamentazione, comprese le autorità nazionali incaricate della protezione dei dati, dovrebbero avere le competenze per imporre azioni inibitorie che impediscano ai trasgressori di proseguire un'attività in violazione della direttiva relativa alla vita privata e alle comunicazioni elettroniche. Le azioni inibitorie o il potere di ordinare la cessazione di una violazione sono strumenti utili nei casi di comportamenti in atto che violano i diritti individuali. Le azioni inibitorie saranno molto utili al fine di porre termine alle violazioni della direttiva relativa alla vita privata e alle comunicazioni elettroniche, ad esempio la violazione dell'articolo 13 sulle comunicazioni commerciali indesiderate, che per sua stessa natura è un comportamento reiterato.

62. In terzo luogo, la proposta consente alla Commissione di adottare misure tecniche di attuazione per assicurare un'efficace collaborazione transfrontaliera nell'applicazione delle norme nazionali (proposta relativa all'articolo 15 *bis*, paragrafo 4). L'esperienza sinora raccolta in materia di cooperazione include l'accordo concluso su iniziativa della Commissione che stabilisce una procedura comune per il trattamento dei reclami transfrontalieri in materia di spam.

([1]) Parere del garante europeo della protezione dei dati sulla comunicazione della Commissione al Parlamento europeo e al Consiglio sul seguito dato al programma di lavoro per una migliore applicazione della direttiva sulla protezione dei dati (GU C 255 del 27.10.2007, pag. 1).

([2]) Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

63. Il GEPD ritiene che se la legislazione sostiene le autorità di regolamentazione che assistono le loro controparti in altri paesi, essa sosterrà sicuramente l'attuazione transfrontaliera. È pertanto opportuno che la proposta consenta alla Commissione di porre in essere le condizioni per garantire la cooperazione transfrontaliera, ivi comprese le procedure per la condivisione di informazioni.

III. **CONCLUSIONI E RACCOMANDAZIONI**

64. Il GEPD esprime piena soddisfazione per la proposta. Le modifiche proposte rafforzano la protezione della vita privata e dei dati personali degli individui nel settore delle comunicazioni elettroniche in maniera non traumatica, che non comporta oneri ingiustificati e inutili per le organizzazioni. Più precisamente, il GEPD ritiene che la maggior parte delle modifiche proposte dovrebbe essere lasciata invariata, in quanto risponde adeguatamente all'obiettivo ricercato. Il punto 69 in appresso elenca le modifiche che il GEDP auspica rimangano invariate.

65. Fatto salvo il giudizio globale positivo sulla proposta, il GEPD ritiene necessario migliorare alcune modifiche, in modo che sia effettivamente prevista una protezione adeguata dei dati personali e della vita privata delle persone. Ciò riguarda in particolare le disposizioni relative alla notifica delle violazioni di sicurezza e quelle concernenti le azioni giudiziarie promosse dai fornitori di servizi di comunicazione elettronica in caso di violazione delle disposizioni in materia di spam. Il GEPD si rammarica inoltre del fatto che la proposta non affronti alcune questioni che non sono trattate in maniera adeguata nella direttiva relativa alla vita privata e alle comunicazioni elettroniche, perdendo l'opportunità di questo riesame per risolvere i problemi ancora insoluti.

66. Per risolvere entrambi i problemi, ossia le questioni che la proposta non affronta adeguatamente e quelle interamente sorvolate, il presente parere ha avanzato alcune proposte redazionali. I punti 67 e 68 espongono in sintesi i problemi e propongono soluzioni redazionali specifiche. Il GEPD invita il legislatore a tenerne conto nell'arco del percorso legislativo della proposta.

67. Le modifiche contenute nella proposta per le quali il GEPD auspica fortemente dei cambiamenti sono le seguenti:

i) **Notifica delle violazioni di sicurezza**: Nella sua attuale formulazione la proposta di modifica che aggiunge *il paragrafo 4 all'articolo 4*, si applica ai fornitori dei servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche (ISP, operatori di rete), che sono obbligati a comunicare alle autorità nazionali di regolamentazione ed ai loro abbonati le violazioni di sicurezza. Il GEPD sostiene pienamente tale obbligo. Il GEPD ritiene tuttavia che l'obbligo dovrebbe applicarsi anche ai fornitori di servizi della società dell'informazione che spesso elaborano informazioni personali sensibili. Le banche e le assicurazioni in linea, i fornitori di servizi sanitari in linea ed altre attività commerciali in linea dovrebbero pertanto conformarsi a tale obbligo.

A tal fine il GEPD propone di inserire, all'articolo 4, paragrafo 3, un riferimento ai fornitori di servizi della società dell'informazione, così formulato: «Se si produce una violazione di sicurezza (…), il fornitore dei servizi di comunicazione elettronica accessibili al pubblico *e il fornitore di servizi della società dell'informazione* comunicano (…) l'avvenuta violazione all'abbonato e all'autorità nazionale di regolamentazione».

ii) **Azioni giudiziarie promosse dai fornitori dei servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche**: Nella sua attuale formulazione, la modifica proposta che aggiunge *il paragrafo 6 all'articolo 13*, introduce la possibilità di ricorsi civili per le persone fisiche o giuridiche, in particolare per i fornitori di servizi di comunicazione elettronica, per lottare contro coloro che violano l'articolo 13 della direttiva relativa alla vita privata e alle comunicazioni elettroniche relativo alle spam. Il GEPD è soddisfatto di tale disposizione. Il GEPD non trova tuttavia logico che questa nuova possibilità sia limitata alle violazioni dell'articolo 13. Suggerisce di consentire alle persone giuridiche di promuovere azioni giudiziarie in caso di violazione di qualsiasi disposizione della direttiva relativa alla vita privata e alle comunicazioni elettroniche.

A questo scopo, il GEPD propone di trasferire il paragrafo 6 dell'articolo 13 in un articolo distinto (articolo 14). Inoltre, il testo dell'articolo 13, paragrafo 6, dovrebbe essere lievemente modificato come segue: invece di «ai sensi del presente articolo» si dovrebbe leggere «ai sensi della presente direttiva».

68. Il campo di applicazione della direttiva relativa alla vita privata e alle comunicazioni elettroniche è attualmente limitato ai fornitori delle reti di comunicazione elettronica accessibili al pubblico; questo è uno degli elementi che la proposta non ha preso in considerazione e che destano maggiore preoccupazione. Il GEPD ritiene necessario modificare la direttiva in modo da ampliarne il campo di applicazione ed includervi i fornitori di servizi di comunicazione elettronica anche su reti miste (pubbliche/private) e private.

69. Il GEPD è assolutamente favorevole a che le modifiche seguenti siano adottate così come sono:

i) **RFID**: La modifica proposta all'*articolo 3*, secondo cui le reti di comunicazione elettronica comprendono le «reti di comunicazione pubbliche che supportano i dispositivi di raccolta e di identificazione dei dati» è pienamente soddisfacente. La disposizione è assai utile poiché chiarisce che una serie di applicazioni RFID deve essere conforme alla direttiva relativa alla vita privata e alle comunicazioni elettroniche, colmando così un certo vuoto giuridico su questo aspetto.

ii) **Cookie/software spia**: La modifica proposta per l'*articolo 5, paragrafo 3*, va accolta con favore poiché l'obbligo di informare e il diritto di opporsi all'installazione di cookie/software spia nel proprio terminale che ne derivano si applicheranno anche nei casi in cui tali dispositivi siano installati mediante supporti esterni per la memorizzazione dei dati quali CD-ROM o chiavi USB. Il GEPD propone tuttavia di apportare una modifica di lieve entità all'ultima parte dell'articolo 5, paragrafo 3, sopprimendo il termine «facilitare».

iii) **Scelta della procedura di comitato con consultazione del GEPD e condizioni/limitazioni dell'obbligo di notifica**: La modifica proposta per l'articolo 4, paragrafo 4, relativa alla notifica delle violazioni di sicurezza, prevede che la decisione su questioni complesse concernenti le circostanze, il formato e le procedure del sistema di notifica sia adottata con procedura di comitato, dopo aver ottenuto il parere del GEPD. Quest'ultimo caldeggia vivamente tale approccio unificato. La legislazione in materia di notifica delle violazioni di sicurezza costituisce un tema a sé stante che occorre affrontare dopo un'analisi e discussioni approfondite.

A questo punto è collegata la richiesta di alcune parti interessate di prevedere all'articolo 4, paragrafo 4, eccezioni all'obbligo di notifica delle violazioni di sicurezza. Il GEPD è fortemente contrario a questo approccio. È per contro favorevole a che il tema della notifica nel suo complesso (modalità, circostanze in cui è possibile abbreviarla o limitarla in qualche modo) sia analizzato globalmente dopo un adeguato dibattito.

iv) **Controllo dell'attuazione**: La modifica proposta, che consiste nell'aggiunta dell'*articolo 15 bis*, contiene molti elementi utili da conservare che contribuiranno a garantire un'osservanza effettiva, tra cui il rafforzamento dei poteri di indagine delle autorità nazionali di regolamentazione (articolo 15 *bis*, paragrafo 3) e la facoltà a queste conferita di disporre la cessazione della violazione.

Fatto a Bruxelles, addì 10 aprile 2008.

Peter HUSTINX

Garante europeo della protezione dei dati