Secondo parere del Garante europeo della protezione dei dati sulla revisione 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)

(2009/C 128/04)

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,

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

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,

HA ADOTTATO IL SEGUENTE PARERE:

I. INTRODUZIONE

Contesto

1. Il 13 novembre 2007, la Commissione europea ha adottato una proposta che modifica, tra l'altro, la direttiva relativa alla vita privata e alle comunicazioni elettroniche, nota anche come direttiva e-privacy [1] (in prosieguo «proposta» o «proposta della Commissione»). Il 10 aprile 2008, il GEPD ha adottato un parere sulla proposta della Commissione in cui forniva raccomandazioni volte a migliorare la proposta nell'intento di contribuire ad assicurare che le modifiche proposte si traducessero nella migliore possibile protezione della vita privata e dei dati delle persone («primo parere del GEPD») [2].

2. Il GEPD ha accolto favorevolmente la proposta della Commissione di istituire un sistema obbligatorio di notificazione delle violazioni di sicurezza che obbliga le società a informare le persone qualora i loro dati personali siano stati compromessi. Ha inoltre elogiato la nuova disposizione che permette alle persone giuridiche (per es. associazioni di consumatori e fornitori di servizi Internet) di promuovere azioni giudiziarie contro i mittenti di comunicazioni commerciali indesiderate (spammer) in modo da integrare ulteriormente gli strumenti esistenti di lotta alle comunicazioni indesiderati.

3. Durante il dibattito parlamentare che ha preceduto la prima lettura del Parlamento europeo, il GEPD ha formulato un ulteriore parere formulando osservazioni su quesiti specifici emersi nelle relazioni redatte dalle commissioni del Parlamento europeo competenti per la revisione delle direttive servizio universale [3] e e-privacy («Osservazioni») [4]. Le osservazioni riguardavano in primo luogo problemi connessi al trattamento di dati relativi al traffico e la protezione dei diritti di proprietà intellettuale.

4. Il 24 settembre 2008, il Parlamento europeo («PE») ha adottato una risoluzione legislativa sulla direttiva e-privacy («prima lettura») [5]. Il GEPD ha valutato positivamente vari emendamenti del PE che sono stati adottati in seguito al parere del GEPD e alle osservazioni succitate. Tra le importanti modifiche figura l'inclusione dei fornitori di servizi della società dell'informazione (ossia le imprese operanti in Internet) nell'ambito di applicazione dell'obbligo di notificare le violazioni di sicurezza. Il GEPD ha anche accolto favorevolmente l'emendamento che

[1] La revisione della direttiva e-privacy è parte di un più ampio processo di riesame inteso alla creazione di un'autorità per le telecomunicazioni a livello di UE, al riesame delle direttive 2002/21/EC, 2002/19/EC, 2002/20/EC, 2002/22/EC e 2002/58/EC, nonché al riesame del regolamento (CE) n. 2006/2004 (in appresso «riesame del pacchetto telecomunicazioni» per l'insieme degli strumenti giuridici).

[2] Parere del 10 aprile 2008 sulla 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 (direttiva relativa alla vita privata e alle comunicazioni elettroniche) GU C 181 del 18.7.2008, pag. 1.

[3] Direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica (direttiva servizio universale), GU L 108, del 24.4.2002, pag. 51.

[4] Osservazioni del GEPD su quesiti specifici emersi dalla relazione IMCO sulla revisione della direttiva 2002/22/EC (servizio universale) e direttiva 2002/58/CE (e-privacy), 2 settembre 2008. Disponibile all'indirizzo: www.edps.europa.eu

[5] Risoluzione legislativa del Parlamento europeo del 24 settembre 2008 sulla 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 [COM(2007) 698 – C6-0420/2007 2007/0248(COD)].

consente alle persone giuridiche e fisiche di promuovere azioni giudiziarie in caso di violazione di qualsiasi disposizione della direttiva e-privacy (non solo in caso di violazione delle disposizioni in materia di spam come proposto inizialmente nella proposta della Commissione). La prima lettura del Parlamento è stata seguita dall'adozione da parte della Commissione di una proposta che modifica la direttiva e-privacy (in prosieguo «proposta modificata») ([6]).

5. Il 27 novembre 2008 il Consiglio ha raggiunto un accordo politico su un riesame delle norme sul pacchetto telecomunicazioni, compresa la direttiva e-privacy, destinato a diventare la posizione comune del Consiglio («posizione comune») ([7]). La posizione comune sarà notificata al PE ai sensi dell'articolo 251, paragrafo 2 del trattato che istituisce la Comunità europea, il che può comportare la proposta di emendamenti da parte del PE.

Parere generale sulla posizione del Consiglio

6. Il Consiglio ha modificato elementi essenziali del testo della proposta e non ha accettato molti degli emendamenti adottati dal PE. È vero che la posizione comune contiene certamente elementi positivi, ma nell'insieme il GEPD è preoccupato per il suo contenuto, in particolare poiché la posizione comune non tiene conto di alcuni degli emendamenti positivi proposti dal PE, della proposta modificata o dei pareri del GEPD e delle autorità europee preposte alla protezione dei dati emessi tramite il gruppo dell'articolo 29 ([8]).

7. Al contrario, in alcuni casi le disposizioni della proposta modificata e degli emendamenti del PE che prevedono garanzie per i cittadini sono state soppresse o indebolite in modo sostanziale. Ne risulta una sostanziale riduzione del livello di protezione offerto alle persone nella posizione comune. Ciò ha indotto il GEPD a emettere un secondo parere, nella speranza che nel corso del processo legislativo sulla direttiva e-privacy siano adottati nuovi emendamenti che ripristinino le garanzie in materia di protezione dei dati.

8. Questo secondo parere è incentrato su alcune preoccupazioni essenziali e non riprende tutti i punti sollevati nel primo parere del GEPD o nelle osservazioni, che rimangono tutti validi. Il presente parere riguarda in particolare i punti seguenti:

— le disposizioni relative alla notifica delle violazioni di sicurezza;

— la portata dell'applicazione della direttiva e-privacy alle reti private e alle reti private accessibili al pubblico;

— il trattamento dei dati relativi al traffico a fini di sicurezza;

— la possibilità offerta alle persone giuridiche di promuovere azioni giudiziarie in caso di violazione della direttiva e-privacy.

9. Nell'affrontare le tematiche succitate, il presente parere analizza la posizione comune del Consiglio e la confronta con la prima lettura del PE e la proposta modificata della Commissione. Il parere contiene raccomandazioni intese a semplificare le disposizioni della direttiva e-privacy e ad assicurare che la direttiva continui a protegge adeguatamente la vita privata e i dati personali.

II. LE DISPOSIZIONI RELATIVE ALLA NOTIFICAZIONE DI VIOLAZIONI DI SICUREZZA

10. Il GEPD sostiene l'adozione di un sistema di notificazione delle violazioni di sicurezza in base al quale alle autorità e alle persone viene data comunicazione qualora i loro dati personali siano stati compromessi ([9]). Le comunicazioni relative a violazioni di sicurezza possono aiutare le persone ad adottare le necessarie misure per attenuare qualsiasi danno potenziale risultante dalla compromissione dei dati. L'obbligo di inviare comunicazioni su violazioni di sicurezza incoraggerà inoltre le società a migliorare la sicurezza dei dati e ad aumentare la loro responsabilità riguardo ai dati personali di cui sono responsabili.

11. La proposta modificata della Commissione, la prima lettura del Parlamento e la posizione comune del Consiglio presentano tre approcci diversi alla notifica di violazioni di sicurezza attualmente all'esame. Ciascuno dei tre approcci ha aspetti positivi. Il GEPD ritiene tuttavia che vi siano possibilità di miglioramento in ciascuno di essi e consiglia di prendere in considerazione le raccomandazioni descritte in appresso nell'esame delle fasi finali in vista dell'adozione di un sistema riguardante le violazioni di sicurezza.

([6]) Proposta modificata 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, Bruxelles 6.11.2008, COM(2008) 723 def.

([7]) Disponibile sul sito web pubblico del Consiglio.

([8]) Parere 2/2008 sul riesame della direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche (direttiva e-privacy), disponibile sul sito web del gruppo dell'articolo 29.

([9]) Nel presente parere è usata la parola «compromessi» in riferimento alle violazioni di dati personali verificatesi in seguito a distruzione, perdita, modifica, rivelazione non autorizzata o accesso, accidentalmente o in modo illecito, in riferimento a dati personali trasmessi, memorizzati o comunque elaborati.

12. Nell'analisi dei tre sistemi di notificazione di violazioni di sicurezza, vanno presi in considerazione cinque punti fondamentali: *i)* la definizione di violazione di sicurezza; *ii)* i soggetti contemplati dall'obbligo di notifica («soggetti contemplati»); *iii)* il criterio che dà luogo all'obbligo di notificazione; *iv)* l'individuazione del soggetto competente per determinare se una violazione di sicurezza soddisfa o non soddisfa il criterio e v) i destinatari dell'informazione.

Panoramica degli approcci della Commissione, del Consiglio e del Parlamento

13. Il Parlamento europeo, la Commissione e il Consiglio hanno adottato differenti approcci per la notificazione di violazioni di sicurezza La prima lettura del PE ha modificato il sistema originario di notificazione di violazioni di sicurezza previsto dalla proposta della Commissione ([10]). In base all'approccio del PE l'obbligo di notificazione non si applica solo ai fornitori di servizi di comunicazione elettronica accessibili al pubblico ma anche ai fornitori di servizi della società dell'informazione («PPECS» e «ISSP»). Inoltre, in base a questo approccio tutte le violazioni di dati personali dovrebbero essere notificate all'autorità nazionale di regolamentazione o alle autorità competenti (insieme «autorità»). Se dovessero determinare che la violazione è *grave*, le autorità competenti richiederebbero ai PPECS e agli ISSP di notificare senza indugio la violazione alle persone che ne sono interessate. In caso di violazioni che rappresentano un pericolo imminente e diretto, i PPECS e gli ISSP informerebbero le persone prima di informare le autorità e non attenderebbero una determinazione normativa. Un'eccezione all'obbligo di informare i consumatori si applica ai soggetti che possono dimostrare alle autorità che sono state applicate appropriate misure di protezione tecnica atte a rendere i dati incomprensibili a chiunque non sia autorizzato ad accedervi.

14. Anche in base all'approccio del Consiglio, la notificazione deve essere fornita sia agli abbonati che alle autorità, ma solo qualora il soggetto contemplato ritenga che la violazione costituisca un rischio grave per la vita privata dell'abbonato (ossia furto o usurpazione d'identità, danno fisico, umiliazione grave o danno alla reputazione).

15. La proposta modificata della Commissione mantiene l'obbligo proposto dal PE di notificare alle autorità tutte le violazioni. Tuttavia, a differenza dell'approccio del Parlamento, la proposta modificata contiene una deroga all'obbligo della notificazione per quanto riguarda le persone interessate qualora il PPECS dimostri all'autorità competente che *i)* «*è ragionevolmente improbabile*» che la violazione comporti una lesione (ad esempio danni economici e sociali o furti di identità) o *ii)* ai dati interessati dalla violazione sono state applicate «*opportune misure di protezione tecnologica*». L'approccio della Commissione include pertanto un'analisi basata sui danni in collegamento con le singole notifiche.

([10]) In particolare, gli emendamenti 187, 124-127 nonché 27, 21 e 32 del PE affrontano tale questione.

16. È importante notare che in base agli approcci del Parlamento ([11]) e della Commissione sono le autorità ad essere in definitiva incaricate di determinare se la violazione sia grave o vi sia una probabilità ragionevole che causi danni. Secondo l'approccio del Consiglio la decisione è invece rimessa ai soggetti interessati.

17. Sia l'approccio del Consiglio che quello della Commissione si applicano soltanto ai PPECS e non, come l'approccio del Parlamento, agli ISSP.

La definizione di violazione di sicurezza

18. Il GEPD è lieto di constatare che le tre proposte legislative contengono la stessa definizione di notifica della violazione di sicurezza descritta come «*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 […]*» ([12]).

19. Come descritto meglio in appresso, questa definizione è accolta favorevolmente in quanto abbastanza generale per abbracciare la maggior parte delle situazioni pertinenti in cui la notificazione di violazioni di sicurezza può essere giustificata.

20. In primo luogo, nella definizione rientrano casi in cui si sia verificato un accesso non autorizzato ai dati personali da parte di terzi, quali la penetrazione in un server contenente dati personali e l'estrazione di tali informazioni.

21. In secondo luogo, la definizione includerebbe anche situazioni in cui si sia verificata la perdita, o la rivelazione di dati personali, anche se l'accesso non autorizzato non è ancora stato dimostrato. Vi rientrerebbero situazioni in cui i dati personali possono essere stati smarriti (per es. CD ROM, chiavi USB o altri dispositivi portatili), o resi disponibili al pubblico da utenti regolari (file di dati sui dipendenti resi inavvertitamente e temporaneamente disponibili in uno spazio accessibile al pubblico via Internet). Poiché spesso non sarà possibile provare che in un determinato momento è o non è possibile che terzi non autorizzati accedano a tali dati o li utilizzino, sembra appropriato includere queste fattispecie nell'ambito della definizione. Il GEPD raccomanda pertanto di mantenere questa definizione. Raccomanda anche di includere la definizione di violazione di sicurezza all'articolo 2 della direttiva e-privacy in quanto ciò sarebbe più coerente con la struttura generale della direttiva e fornirebbe maggiore chiarezza.

([11]) Eccetto qualora esista un pericolo imminente e diretto, nel qual caso i soggetti contemplati devono informare prima i consumatori.

([12]) Articolo 2, lettera i) della posizione comune e della proposta modificate e articolo 3, paragrafo 3 della prima lettura del Parlamento.

Soggetti ai quali dovrebbe essere imposto l'obbligo della notificazione

22. In base all'approccio del PE, l'obbligo di notificazione si applica sia ai PPECS che agli ISSP. Tuttavia, secondo i regimi previsti dal Consiglio e dalla Commissione, solo PPECS quali le società di telecomunicazione e i fornitori di accesso a Internet saranno obbligati a informare le persone qualora subiscano violazioni di sicurezza che comportano la compromissione di dati personali. Altri settori di attività, per esempio le banche in linea, i rivenditori in linea, i fornitori di servizi sanitari in linea e altri non sono vincolati da questo obbligo. Per i motivi succitati, il GEPD ritiene che dal punto di vista dell'interesse pubblico sia fondamentale assicurare che anche i servizi della società dell'informazione che includono il commercio in linea, le banche in linea, i fornitori di servizi sanitari in linea ecc. siano soggetti all'obbligo di notificazione.

23. In primo luogo, il GEPD rileva che benché le società di telecomunicazione siano certamente oggetto di violazioni di sicurezza che giustificano un obbligo di notificazione, lo stesso vale per altri tipi di società/fornitori. Anche i rivenditori in linea, le banche in linea, le farmacie in linea possono subire violazioni di sicurezza alla stessa stregua delle società di telecomunicazione, se non in misura maggiore. Pertanto, considerato il rischio, non è opportuno limitare ai PPECS l'obbligo di notificazione di una violazione. L'esigenza di un approccio più ampio è corroborato dalle esperienze acquisite in altri paesi. Per esempio, negli Stati Uniti quasi tutti gli Stati (attualmente oltre 40) hanno varato leggi sulla notificazione di violazioni di sicurezza che hanno un campo d'applicazione più ampio, che comprende non solo i PPECS ma qualsiasi soggetto che detiene i dati personali richiesti.

24. In secondo luogo, se una violazione dei tipi di dati personali regolarmente trattati dai PPECS può chiaramente incidere sulla vita privata di una persona, lo stesso vale, forse a maggior ragione, per i tipi di informazioni trattate dagli ISSP. Certamente le banche e altri istituti finanziari possono essere in possesso di informazioni altamente riservate (per es. dettagli di conti bancari), la cui divulgazione può dar luogo a un uso a fini di usurpazione dell'identità. Anche la divulgazione di informazioni assai sensibili attinenti alla salute da parte di servizi sanitari in linea può essere particolarmente dannosa per le persone. Pertanto, anche i tipi di dati personali che possono essere compromessi richiedono una più ampia applicazione della notificazione di violazione di sicurezza che includerebbe, come minimo, gli ISSP.

25. Sono stati sollevati alcuni problemi di natura giuridica riguardo all'ampliamento del campo d'applicazione di questo articolo, ossia i soggetti contemplati dall'obbligo in questione. In particolare il fatto che il campo d'applicazione generale della direttiva e-privacy riguardi solo i PPECS è stato addotto come ostacolo all'applicazione dell'obbligo di notificare anche agli ISSP.

26. In questo contesto il GEPD tiene a ricordare quanto segue: *i)* non esiste nessun tipo di ostacolo all'inclusione di attori diversi dai PPECS nel campo di applicazione di determinate disposizioni della direttiva. Il legislatore comunitario dispone di un potere discrezionale illimitato a tale riguardo; *ii)* nella vigente direttiva e-privacy esistono altri precedenti di applicazione a soggetti diversi dai PPECS.

27. Per esempio, l'articolo 13 si applica non solo ai PPECS ma a qualsiasi società che invia comunicazioni non richieste, prescrivendo un consenso «opt-in» preliminare a tal fine. Inoltre, l'articolo 5, paragrafo 3 della direttiva e-privacy che vieta, tra l'altro, la memorizzazione di informazioni quali cookie nei terminali degli utenti è vincolante non solo per i PPECS ma anche per chiunque tenti di memorizzare informazioni o ottenere l'accesso alle informazioni memorizzate nell'apparecchiatura terminale delle persone. Per giunta, nel processo legislativo in corso, la Commissione ha addirittura proposto di estendere l'applicazione dell'articolo 5, paragrafo 3 ai casi in cui tecnologie analoghe (cookie/software spia) siano forniti non solo tramite sistemi di comunicazione elettronica ma anche tramite qualsiasi altro metodo possibile (distribuzione attraverso software provenienti da Internet oppure attraverso supporti esterni per la memorizzazione dei dati, quali CD-ROM, chiavi USB, unità flash ecc.). Tutti questi elementi sono positivi e dovrebbero essere mantenuti, ma anche costituire precedenti per l'attuale discussione sul campo d'applicazione.

28. Inoltre, nell'attuale processo legislativo, la Commissione e il PE e presumibilmente il Consiglio hanno proposto un nuovo articolo 6, paragrafo 6, lettera a) discusso in appresso, che si applica a soggetti diversi dai PPECS.

29. Infine, tenuto conto degli elementi generalmente positivi derivanti dall'obbligo di notificare violazioni di sicurezza, è molto probabile che i cittadini si aspettino questi vantaggi non solo qualora i loro dati personali siano stati compromessi da PPECS ma anche qualora ciò sia avvenuto ad opera di ISSP. Le attese dei cittadini potrebbero essere deluse se, ad esempio, non venissero informati qualora una banca in linea abbia smarrito le informazioni sul loro conto bancario.

30. In definitiva, il GEPD è convinto che la notificazione di violazioni di sicurezza potrà produrre tutti i suoi effetti positivi solo se i soggetti contemplati comprenderanno sia i PPECS che gli ISSP.

Il criterio che dà luogo alla notificazione

31. Per quanto riguarda l'attivazione della notificazione, come spiegato dettagliatamente in appresso, il GEPD ritiene che il criterio della proposta modificata «*ragionevolmente probabile che possa ledere*» sia il più appropriato dei tre criteri proposti. Tuttavia, è importante far sì che il concetto di «ledere» sia sufficientemente ampio da contemplare tutte le pertinenti fattispecie di effetti negativi sulla vita privata o su altri interessi legittimi delle persone. Altrimenti sarebbe preferibile introdurre un nuovo criterio in base al quale la notificazione sarebbe obbligatoria «*se vi è una probabilità ragionevole che la violazione produca effetti negativi per le persone*».

32. Come accennato nella sezione precedente, le condizioni alle quali deve essere data comunicazione alle persone (denominati «attivazione» e «criterio») sono diversi nell'ambito degli approcci del PE, della Commissione e del Consiglio. È ovvio che la quantità delle comunicazioni che le persone riceveranno dipenderà, in larga misura, dall'attivazione o dal criterio fissati per la notificazione.

33. In base all'approccio del Consiglio e della Commissione, la notificazione deve essere effettuata se la violazione costituisce una «grave violazione della vita privata dell'abbonato» (Consiglio) e se «*è ragionevolmente probabile che la violazione possa ledere gli interessi del consumatore*» In base all'approccio del PE, l'attivazione per la notificazione alle persone è data dalla «gravità della violazione» (ossia la notifica alle persone è richiesta se la violazione è considerata «grave»). Al di sotto di tale soglia non è necessaria la notificazione ([13])

34. Il GEPD comprende che si può sostenere che, se sono stati compromessi dati personali, le persone ai quali appartengono i dati hanno il diritto di venirne a conoscenza in qualsiasi circostanza. Ma è corretto ponderare se ciò sia una soluzione appropriata alla luce di altri interessi e considerazioni.

35. È stato affermato che l'obbligo di inviare comunicazioni ogniqualvolta siano stati compromessi dati personali, in altre parole senza limitazioni, può comportare un eccesso di notificazioni e «stanchezza da comunicazioni» il che potrebbe tradursi in desensibilizzazione. Come precisato in appresso, il GEPD è sensibile a questo argomento; tuttavia tiene a sottolineare la sua preoccupazione per il fatto che l'eccesso di notificazioni è un possibile indicatore di diffuse carenze nelle prassi in materia di sicurezza dell'informazione.

([13]) Cfr. nota 11 relativa alla deroga a tale norma.

36. Come indicato in precedenza, il GEPD ravvisa potenziali conseguenze negative nell'eccesso di notificazioni e desidera contribuire ad assicurare che il quadro giuridico adottato per la notificazione di violazioni di sicurezza non produca questo risultato. Se le persone dovessero ricevere frequenti comunicazioni di violazione anche in situazioni in cui non vi sono effetti negativi, danni o pericoli, può andare a finire che venga messo a repentaglio uno degli obiettivi fondamentali della comunicazione in quanto, paradossalmente, le persone potrebbero ignorare comunicazioni in casi in cui potrebbero effettivamente dover intervenire per proteggersi. È quindi importante trovare un giusto equilibrio nel fornire comunicazioni sensate poiché, se le persone non reagiscono alle comunicazioni ricevute, l'efficacia dei sistemi di notificazione è fortemente ridotta.

37. Al fine di adottare un criterio appropriato che non porti a un eccesso di notificazioni, vanno esaminati, oltre all'attivazione della comunicazione, altri fattori, in particolare la definizione di violazione di sicurezza e l'informazione oggetto dell'obbligo di notificazione. A tale riguardo il GEPD rileva che in base ai tre approcci proposti, è possibile avere una gran quantità di notificazioni tenuto conto dell'ampia definizione di violazione di sicurezza succitata. Questa preoccupazione per un eccesso di notificazioni è ulteriormente sottolineata dal fatto che la definizione di violazione di sicurezza si applica a tutti i tipi di dati personali. Benché il GEPD ritenga che questo sia l'approccio corretto (che non limita i tipi di dati personali soggetti a notificazione), contrariamente ad altri approcci quali le leggi USA in cui i requisiti sono incentrai sulla sensibilità dell'informazione, si tratta comunque di un fattore di cui tener conto.

38. Alla luce di quanto indicato sopra e tenendo conto delle diverse variabili esaminate nel loro insieme, il GEPD ritiene appropriato includere una soglia o criterio al di sotto del quale la notificazione non è obbligatoria.

39. I criteri proposti secondo cui la violazione deve rappresentare un «*rischio grave per la vita privata*» o è «*ragionevolmente probabile che possa ledere*» sembrano entrambi includere, per esempio, danni sociali, alla reputazione o economici. Per esempio questi criteri riguarderebbero casi di esposizione a usurpazione dell'identità mediante la divulgazione di identificatori non pubblici quali i numeri di passaporto, nonché la rivelazione di informazioni sulla vita privata di una persona. Il GEPD è favorevole a questa impostazione. È convinto che non sarebbero realizzati tutti i possibili effetti positivi della notificazione di violazioni di sicurezza se il sistema di notificazione contemplasse solo le violazioni che comportano danni economici.

40. Tra i due criteri proposti, il GEPD preferisce il criterio proposto dalla Commissione «*ragionevolmente probabile che possa ledere*» in quanto offrirebbe un livello più appropriato di protezione delle persone. È molto più probabile che le violazioni giustifichino una notificazione qualora sia «*ragionevolmente probabile che possano ledere*» la vita privata delle persone che qualora presentino «*un grave rischio*» di lesione. Pertanto, contemplando solo le violazioni che presentano un grave rischio per la vita privata delle persone si limiterebbe considerevolmente il numero delle violazioni che devono essere notificate. Contemplando solo questo genere di violazioni si conferirebbe ai PPECS e agli ISSP un potere discrezionale smodato per quanto riguarda la necessità di emettere una notificazione, in quanto sarebbe molto più facile per loro giustificare la conclusione secondo cui non esiste «nessun *rischio grave*» che la conclusione secondo cui è «*ragionevolmente improbabile che si verifichi*» una lesione. È vero che occorre comunque evitare un eccesso di notifiche, ma in compenso deve essere concesso il beneficio del dubbio al fine di proteggere l'interesse delle persone alla loro vita privata e il limite minimo per la protezione delle persone è dato dal momento in cui è ragionevolmente probabile che una violazione causi loro dei danni. Inoltre i termini «*ragionevolmente probabile*» saranno più efficaci nell'applicazione pratica, sia per i soggetti contemplati che per le autorità competenti, in quanto richiedono una valutazione oggettiva del caso e del relativo contesto.

41. Le violazioni riguardanti dati personali possono inoltre creare danni che sono difficilmente quantificabili e possono essere di diversa natura. Infatti, la divulgazione dello stesso tipo di dati può, a seconda delle circostanze specifiche, provocare danni significativi a una persona e minori a un'altra. Non sarebbe appropriato un criterio secondo cui il danno deve essere materiale, significativo o grave. Per esempio, l'approccio del Consiglio secondo cui la violazione deve pregiudicare *gravemente* la vita privata di una persona, fornirebbe una protezione inadeguata ai singoli nella misura in cui tale criterio richiede che l'effetto sulla vita privata sia «grave». Ciò dà altresì adito a una valutazione soggettiva.

42. Mentre, come precedentemente descritto, il criterio: «*ragionevolmente probabile che possa ledere*» sembra essere appropriato per la notificazione di violazione di sicurezza, il GEPD continua a nutrire la preoccupazione che esso non possa includere tutte le situazioni in cui è giustificata una comunicazione alle persone, ossia tutte le situazioni in cui vi è una probabilità ragionevole di effetti negativi sulla vita privata o su altri interessi legittimi delle persone. Per tale motivo potrebbe essere preso in considerazione un criterio che darebbe luogo alla notificazione «*se vi è una probabilità ragionevole che la violazione produca effetti negativi per le persone*».

43. Questo criterio alternativo presenta l'ulteriore vantaggio della conformità alla normativa dell'UE in materia di protezione dei dati. In effetti, la direttiva sulla tutela dei dati fa spesso riferimento ad effetti negativi sui diritti e le libertà degli interessati. Per esempio, l'articolo 18 e il considerando 49, che riguardano l'obbligo di registrare le operazioni di trattamento dei dati presso le autorità preposte alla protezione dei dati, autorizzano gli Stati membri a derogare a tale obbligo qualora i trattamenti non siano «*tali da recare pregiudizio ai diritti e alle libertà delle persone interessate*» Termini analoghi figurano all'articolo 16, paragrafo 6 della posizione comune che autorizza le persone giuridiche a promuovere azioni giudiziarie contro coloro che inviano messaggi di posta elettronica indesiderata (spammer).

44. Inoltre, tenendo conto di quanto precede, ci si aspetterebbe anche che i soggetti contemplati e in particolare le autorità competenti a mettere in atto la normativa in materia di protezione dei dati avessero maggiore familiarità con il criterio suddetto, facilitando in tal modo la valutazione se una determinata violazione soddisfi il criterio previsto.

Soggetto competente per determinare se una violazione di sicurezza soddisfa o non soddisfa il criterio

45. In base all'approccio del PE (fatta eccezione per i casi di pericolo imminente) e alla proposta modificata della Commissione, spetta alle autorità degli Stati membri determinare se una violazione di sicurezza soddisfi il criterio di attivazione dell'obbligo di notificazione agli interessati.

46. Il GEPD ritiene che il coinvolgimento di un'autorità svolga un ruolo importante nel determinare se un criterio è soddisfatto in quanto ciò è, in una certa misura, una garanzia per la corretta applicazione della legge. Questo sistema può impedire che le società, in modo inappropriato, considerino la violazione non lesiva/grave evitando in tal modo la notificazione allorché, in effetti, tale notificazione è necessaria.

47. D'altro canto, il GEPD nutre preoccupazione per il fatto che un regime secondo il quale le autorità sono incaricate di effettuare la valutazione può essere poco pratico e di difficile applicazione, o può nella prassi rivelarsi controproducente. Può addirittura diminuire le garanzie in materia di protezione dei dati per le persone.

48. Infatti, in base a tale approccio le autorità preposte alla protezione dei dati verranno probabilmente inondate da notificazioni di violazioni di sicurezza e potranno incontrare gravi difficoltà nell'effettuare le necessarie valutazioni. È importante ricordare che per valutare se una violazione soddisfa il criterio previsto, le autorità dovranno disporre di sufficienti informazioni interne, spesso di natura tecnica complessa, che dovranno trattare molto rapidamente. Tenendo conto della difficoltà di valutazione e del fatto che alcune autorità dispongono di risorse limitate, il GEPD teme che sarà assai difficile per le autorità adempiere a questo obbligo e che saranno loro sottratte risorse necessarie per altre priorità importanti. Inoltre, tale sistema può esercitare un'indebita pressione sulle autorità; in effetti, se esse decidono che la violazione non è grave e ciò nonostante le persone subiscono dei danni, le autorità potrebbero essere ritenute responsabili.

49. Questa difficoltà è ulteriormente evidenziata se si tiene conto del fatto che il tempo è un fattore determinante nel ridurre al minimo i rischi derivanti da violazioni di sicurezza. A meno che le autorità siano in grado di effettuare la valutazione entro un lasso di tempo assai breve, l'ulteriore tempo richiesto affinché le autorità possano effettuare tali valutazioni può aumentare i danni subiti dagli interessati. Pertanto, questo intervento aggiuntivo che è inteso a fornire una maggiore protezione alle persone può, paradossalmente, tradursi in una minore protezione rispetto ai sistemi basati sulla notificazione diretta.

50. Per i motivi succitati, il GEPD ritiene che sia preferibile istituire un sistema secondo il quale spetterebbe ai soggetti interessati valutare se la violazione soddisfi o non soddisfi il pertinente criterio, come previsto nell'approccio del Consiglio.

51. Tuttavia, per evitare rischi di possibili abusi, per esempio da parte di soggetti che rifiutano la notificazione in circostanze in cui essa è chiaramente dovuta, è estremamente importante includere determinate garanzie in materia di protezione dei dati che sono descritte in appresso

52. In primo luogo, l'obbligo imposto ai soggetti contemplati di determinare se devono effettuare la notificazione deve evidentemente essere accompagnato da un altro obbligo relativo alla notificazione obbligatoria alle autorità di tutte le violazioni che soddisfano il criterio stabilito. I soggetti interessati dovrebbero in questi casi essere obbligati a informare le autorità della violazione e dei motivi della loro decisione riguardante la notificazione nonché del contenuto di tutte le notificazioni effettuate.

53. In secondo luogo, alle autorità deve essere conferito un effettivo ruolo di supervisione. Nell'esercitare questo ruolo, le autorità devono avere la facoltà, ma non l'obbligo, di indagare sulle circostanze della violazione e imporre qualsiasi misura necessaria per porvi rimedio ([14]). Ciò dovrebbe includere non solo la comunicazione alle persone (se non ha già avuto luogo) ma anche la facoltà di imporre l'obbligo di intervenire per impedire ulteriori violazioni. Alle autorità dovrebbero essere attribuiti effettivi poteri e risorse a tale riguardo nonché il necessario margine di discrezionalità per decidere quando reagire a una notificazione riguardante una violazione di sicurezza. In altre parole, ciò consentirebbe alle autorità di essere selettive ed effettuare indagini su, per esempio, violazioni di sicurezza di vasta portata e veramente dannose, verificando e imponendo l'ottemperanza a quanto prescrive la legge.

54. Per conseguire l'obiettivo succitato, in aggiunta ai poteri conferiti dalla direttiva e-privacy nonché dall'articolo 15 bis, paragrafo 3 e dalla direttiva sulla tutela dei dati, il GEPD raccomanda di inserire il testo seguente: «*Se l'abbonato o il singolo interessato non ha ancora ricevuto la notificazione, le autorità nazionali competenti, considerata la natura della violazione, possono chiedere ai PPECS o agli ISSP di provvedere alla notificazione*».

55. Il GEPD raccomanda inoltre al PE e al Consiglio di confermare l'obbligo proposto dal PE (emendamento 122, articolo 4, paragrafo 1, lettera a) che i soggetti effettuino una valutazione e identificazione dei rischi riguardo ai loro sistemi e ai dati personali che intendono trattare. In base a questo obbligo, i soggetti dovrebbero elaborare una definizione adeguata e accurata delle misure di sicurezza che saranno applicate nei casi che li riguardano, che dovrebbe essere a disposizione delle autorità. In caso di violazione di sicurezza, questo obbligo aiuterà i soggetti contemplati — e in definitiva anche le autorità nell'espletamento della loro funzione di supervisione — a determinare se la compromissione di tali informazioni può provocare effetti negativi o danni alle persone.

56. In terzo luogo, l'obbligo imposto ai soggetti contemplati di determinare se devono effettuare notificazioni alle persone deve essere accompagnato da un obbligo di mantenere piste di controllo interno dettagliate e globali con la descrizione di tutte le violazioni verificatesi e di tutte le relative notificazioni nonché di tutte le misure prese per evitare future violazioni. Queste piste di controllo interno devono essere a disposizione delle autorità per l'esame e le eventuali indagini. Ciò consentirà alle autorità di espletare le loro funzioni di supervisione. Ciò potrebbe essere conseguito con l'adozione di un testo del tenore seguente: «*I PPECS e gli ISSP effettuano e conservano una registrazione completa e dettagliata di tutte le violazioni di sicurezza occorse, delle pertinenti informazioni tecniche ad esse collegate e delle misure adottate per porvi rimedio. I registri contengono altresì un riferimento a tutte le notificazioni effettuate agli abbonati o ai singoli interessati nonché alle autorità nazionali competenti, inclusi le relative date e il relativo contenuto. I registri sono prodotti all'autorità nazionale competente a sua richiesta*».

57. Naturalmente, al fine di assicurare la coerenza nell'attuazione di questa norma nonché di altri aspetti pertinenti del quadro relativo alla violazione di sicurezza, come il formato e la procedura per la notificazione, è opportuno che la Commissione adotti misure tecniche di attuazione, previa consultazione del GEPD, del Gruppo dell'articolo 29 e di altri pertinenti soggetti interessati.

([14]) L'articolo 15 bis, paragrafo 3 riconosce questa facoltà di supervisione prevedendo che «*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*».

Destinatari della notificazione

58. Per quanto riguarda i destinatari delle comunicazioni, il GEPD preferisce il testo del PE e della Commissione a quello del Consiglio. In effetti il PE ha sostituito la parola «abbonati» con la parola «utenti». La Commissione usa «abbonati» e «singoli interessati». Sia il testo del PE che quello della Commissione includerebbero come destinatari delle comunicazioni non solo gli abbonati ma anche precedenti abbonati e terzi, quali gli utenti che interagiscono con determinati soggetti contemplati senza avere un abbonamento. Il GEPD accoglie favorevolmente questo approccio e invita il PE e il Consiglio a mantenerlo.

59. Tuttavia, il GEPD rileva alcune incoerenze terminologiche nella prima lettura del PE che andrebbero rimosse. Per esempio, la parola «abbonati» è stata sostituita nella maggior parte dei casi, ma non sempre, con la parola «utenti», in altri casi con «consumatori». In questi casi è necessaria un'armonizzazione.

III. **CAMPO DI APPLICAZIONE DELLA DIRETTIVA E-PRIVACY: RETI PUBBLICHE E PRIVATE**

60. L'articolo 3, paragrafo 1 della vigente direttiva e-privacy determina i soggetti principalmente interessati dalla direttiva, ossia coloro che effettuano il trattamento dei dati «*connesso alla*» fornitura di servizi pubblici di comunicazione elettronica su reti pubbliche (sopra indicati come «PPECS») ([15]). Tra gli esempi delle attività dei PPECS figurano la fornitura di accesso a Internet, la trasmissione di informazioni attraverso reti elettroniche, le connessioni telefoniche fisse e mobili, ecc.

61. Il Parlamento europeo ha votato l'emendamento 121 che modifica l'articolo 3 della proposta iniziale della Commissione, in base al quale il campo di applicazione della direttiva e-privacy è stato ampliato al fine di includere «*il trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche e private e su reti private accessibili al pubblico nella Comunità, […]*» (art. 3, paragrafo 1 della direttiva e-privacy). Purtroppo il Consiglio e la Commissione hanno avuto difficoltà ad accettare questo emendamento e non hanno pertanto integrato tale approccio nella posizione comune e nella proposta modificata.

Applicazione della direttiva e-privacy alle reti private accessibili al pubblico

62. Per i motivi illustrati in appresso e al fine di contribuire a promuovere un consenso, il GEPD invita a preservare la sostanza dell'emendamento 121. Inoltre, il GEPD suggerisce di includere un emendamento che contribuisca a precisare ulteriormente i tipi di servizi che rientrerebbero nel campo di applicazione ampliato.

([15]) «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».

63. Le reti private sono spesso utilizzate per fornire servizi di comunicazione elettronica quali l'accesso a Internet a un numero indeterminato di persone, potenzialmente elevato. Ciò si verifica ad esempio per l'accesso a Internet negli Internet café come pure nei punti Wi-Fi disponibili in alberghi, ristoranti, aeroporti, treni e in altri stabilimenti aperti al pubblico, ove siffatti servizi sono spesso forniti a complemento di altri servizi (bevande, alloggio, ecc.).

64. In tutti i summenzionati casi, un servizio di comunicazione, ad esempio l'accesso a Internet, è messo a disposizione del pubblico non attraverso una rete pubblica bensì attraverso quella che può essere considerata una rete privata, ossia una rete gestita privatamente. Inoltre, sebbene nei casi succitati il servizio di comunicazione sia fornito al pubblico, poiché il tipo di rete utilizzato è privato anziché pubblico, *si può sostenere che* la fornitura di tali servizi non è contemplata dall'intera direttiva e-privacy o almeno da alcuni dei suoi articoli ([16]). Conseguentemente, i diritti fondamentali dei singoli garantiti dalla direttiva e-privacy non sono protetti in tali casi e si crea una situazione giuridica di squilibrio tra gli utenti che accedono ai medesimi servizi Internet attraverso mezzi di telecomunicazione pubblici e gli utenti che vi accedono attraverso mezzi di telecomunicazione privati. Ciò si verifica nonostante il livello di rischio per la tutela della vita privata e dei dati personali in tutti questi casi sia pari a quello connesso all'utilizzo di reti pubbliche per la trasmissione del servizio. In sintesi, non sembra esistere una giustificazione *razionale* per un trattamento differenziato, ai sensi della direttiva, dei servizi di comunicazione forniti tramite una rete privata rispetto a quelli forniti tramite una rete pubblica.

65. Pertanto il GEPD sarebbe favorevole ad un emendamento, quale l'emendamento 121 del PE, secondo cui la direttiva e-privacy si applicherebbe parimenti al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione *private*.

66. Il GEPD riconosce tuttavia che una siffatta formulazione potrebbe comportare conseguenze imprevedibili ed eventualmente non volute. In realtà, il semplice riferimento alle reti private potrebbe essere interpretato come tale da contemplare situazioni che chiaramente non si intende

([16]) *A contrario*, si potrebbe sostenere che, poiché il servizio di comunicazione è fornito al pubblico, anche se la rete è privata, la fornitura di tali servizi è contemplata dal quadro giuridico esistente malgrado il fatto che la rete sia privata. In realtà, ad esempio, in Francia i datori di lavoro che forniscono ai loro impiegati un accesso a Internet sono stati considerati soggetti equivalenti ai fornitori di servizi Internet che offrono un accesso a Internet su base commerciale. Tale interpretazione non è ampiamente accettata.

contemplare nella direttiva. Ad esempio, si potrebbe affermare che un'interpretazione letterale o rigorosa di tale formulazione potrebbe far rientrare nel campo di applicazione della direttiva i proprietari di case dotate di tecnologia Wi-Fi ([17]), che consente la connessione a chiunque si trovi entro il suo raggio d'azione (che comprende solitamente la casa), benché non sia questo il proposito dell'emendamento 121. Al fine di evitare tale risultato, il GEPD suggerisce di riformulare l'emendamento 121 facendo rientrare nel campo di applicazione della direttiva e-privacy «*il trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche o private accessibili al pubblico nella Comunità,…*».

67. Ciò contribuirebbe a chiarire che solo le reti private accessibili al pubblico sarebbero contemplate dalla direttiva e-privacy. Applicando le disposizioni della direttiva e-privacy *unicamente* alle *reti private accessibili al pubblico* (e non a tutte le reti private) si stabilisce un limite, di modo che la direttiva contempli soltanto i servizi di comunicazione forniti su reti private che sono intenzionalmente resi *accessibili* al pubblico. Tale formulazione contribuirà a sottolineare ulteriormente che *la disponibilità* delle reti private *per i membri del grande pubblico* costituisce il fattore essenziale per determinare se queste ultime sarebbero contemplate dalla direttiva (oltre alla fornitura di un servizio di comunicazione accessibile al pubblico). In altri termini, a prescindere dal fatto che la rete sia pubblica o privata, se la rete è intenzionalmente resa disponibile al pubblico al fine di fornire un servizio pubblico di comunicazione, quale l'accesso a Internet, anche se tale servizio è complementare a un altro servizio (ad es. la sistemazione alberghiera), questo tipo di servizio/rete rientrerà nel campo di applicazione della direttiva e-privacy.

68. Il GEPD rileva che l'approccio sopra caldeggiato, secondo il quale le disposizioni della direttiva e-privacy si applicano alle *reti private accessibili al pubblico*, è coerente con le impostazioni adottate in diversi Stati membri, le cui autorità hanno già considerato che tale tipo di servizi come pure i servizi forniti su reti esclusivamente private rientrino nel campo di applicazione delle disposizioni nazionali di attuazione della direttiva e-privacy ([18]).

69. Ai fini di una maggiore certezza del diritto in merito ai soggetti rientranti nel nuovo campo di applicazione, potrebbe essere utile includere nella direttiva e-privacy una modifica che definisca le «reti private accessibili al pubblico», del seguente tenore: «*"rete privata accessibile al pubblico": una rete gestita privatamente alla quale i membri del grande pubblico hanno di norma accesso senza restrizioni, a pagamento o gratuitamente o in connessione con altri servizi o offerte, fatta salva l'accettazione delle condizioni e modalità applicabili.*»

70. In pratica, secondo l'approccio sopra indicato le reti private negli alberghi ed altri stabilimenti che forniscono l'accesso a Internet al grande pubblico tramite una rete privata rientrerebbero nel campo di applicazione. Per contro, la fornitura di servizi di comunicazione su reti esclusivamente private, ove il servizio è limitato a un gruppo ristretto di persone identificabili, non sarebbe contemplata. Pertanto, ad esempio, le reti private virtuali e le case di consumatori dotate di tecnologia Wi-Fi non sarebbero contemplate dalla direttiva. Neppure i servizi forniti tramite reti esclusivamente d'impresa sarebbero contemplati.

Reti private rientranti nel campo di applicazione della direttiva e-privacy

71. L'esclusione delle reti private in quanto tali sopra suggerita dovrebbe essere considerata una misura provvisoria, da discutere ulteriormente. In realtà, in considerazione, da un lato, delle implicazioni in materia di tutela della vita privata derivanti dall'esclusione delle reti puramente private e, d'altro lato, del fatto che tale esclusione interessa un gran numero di persone che accedono abitualmente ad Internet tramite reti d'impresa, tale questione dovrà forse essere riesaminata in futuro. Per questo motivo, e al fine di incentivare il dibattito su tale argomento, il GEPD raccomanda di includere nella direttiva e-privacy un considerando secondo cui la Commissione effettuerà una consultazione pubblica sull'applicazione della direttiva e-privacy a tutte le reti private, con il contributo del GEPD, delle autorità preposte alla protezione dei dati e di altri pertinenti soggetti interessati. Inoltre, il considerando potrebbe precisare che, a seguito della consultazione pubblica, la Commissione dovrebbe presentare proposte appropriate per estendere o limitare i tipi di soggetti che dovrebbe essere contemplati dalla direttiva e-privacy.

72. A complemento di quanto sopra indicato, i diversi articoli della direttiva e-privacy dovrebbero essere modificati di conseguenza, di modo che tutte le disposizioni operative menzionino esplicitamente le reti private disponibili al pubblico oltre alle reti pubbliche.

IV. **TRATTAMENTO DEI DATI RELATIVI AL TRAFFICO A FINI DI SICUREZZA**

73. Durante l'iter legislativo relativo al riesame della direttiva e-privacy, le società fornitrici di servizi di sicurezza hanno ribadito la necessità di introdurre nella suddetta direttiva una disposizione intesa a legittimare la raccolta di dati relativi al traffico al fine di garantire un'effettiva sicurezza in linea.

([17]) Typically wireless Local Area Networks (reti locali tipicamente senza fili) (LAN).

([18]) Cfr. nota a piè di pagina 16.

74. Di conseguenza, il PE ha introdotto l'emendamento 181, che ha creato un nuovo articolo 6, paragrafo 6 bis, che autorizza esplicitamente il trattamento di dati relativi al traffico a fini di sicurezza: «*Senza pregiudizio per il rispetto delle disposizioni diverse dall'articolo 7 della direttiva 95/46/CE e dall'articolo 5 della presente direttiva, i dati possono essere trattati per il legittimo interesse del responsabile del trattamento al fine di applicare misure tecniche intese a garantire la sicurezza della rete e dell'informazione, quali definiti 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, di un servizio pubblico di comunicazione elettronica, una rete pubblica o privata di comunicazioni elettroniche, un servizio della società dell'informazione o relativo terminal e dispositivo elettronico di comunicazione, salvo ove su tali interessi prevalgano gli interessi per i diritti e le libertà fondamentali della persona interessata. Tale trattamento deve limitarsi allo stretto necessario ai fini di tale attività di sicurezza.*»

75. La Commissione, nella sua proposta modificata, ha accettato tale emendamento in linea di principio ma, eliminando la clausola che recita: «*Senza pregiudizio […] della presente direttiva*», ha eliminato una clausola fondamentale, intesa ad assicurare il rispetto delle altre disposizioni della direttiva. Il Consiglio ha adottato una versione riformulata, che si è spinta ancora oltre nell'affievolire gli importanti elementi di protezione e di equilibrio degli interessi che erano parte integrante dell'emendamento 181, adottando la seguente formulazione: «*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*».

76. Come ulteriormente precisato in appresso, l'articolo 6, paragrafo 6 bis è superfluo e soggetto al rischio di abuso, in particolare se adottato in una formulazione che non includa le importanti garanzie, le clausole che assicurino il rispetto delle altre disposizioni della direttiva e l'equilibrio degli interessi. Pertanto il GEPD raccomanda di respingere tale articolo o quanto meno di provvedere a che qualsiasi articolo siffatto in materia comprenda i tipi di garanzie inclusi nell'emendamento 181 adottato dal PE.

Motivazioni giuridiche del trattamento dei dati relativi al traffico applicabili ai servizi di comunicazione elettronica e ad altri responsabili del trattamento ai sensi della vigente normativa sulla protezione dei dati

77. La misura in cui i fornitori di servizi di comunicazione elettronica accessibili al pubblico possono legalmente trattare i dati relativi al traffico è disciplinata a norma dell'articolo 6 della direttiva e-privacy, che limita il trattamento dei dati relativi al traffico ad una serie circoscritta di finalità quali la fatturazione, l'interconnessione e la commercializzazione. Tale trattamento può aver luogo soltanto fatte salve determinate condizioni, quali il consenso delle persone interessate nel caso della commercializzazione. Inoltre, altri responsabili del trattamento quali i fornitori di servizi della società dell'informazione possono trattare i dati relativi al traffico a norma dell'articolo 7 della direttiva sulla tutela dei dati, che stabilisce che i responsabili del trattamento possono effettuare il trattamento di dati personali se soddisfano almeno una delle basi giuridiche elencate, menzionate anche come motivazioni giuridiche.

78. Un esempio di siffatte basi giuridiche è costituito dall'articolo 7, lettera a), della direttiva sulla tutela dei dati, che richiede il consenso della persona interessata. Ad esempio, se un rivenditore in linea intende trattare dati relativi al traffico al fine di pubblicizzare o commercializzare del materiale, deve ottenere il consenso della persona interessata. Un'altra base giuridica stabilita all'articolo 7 può consentire, in taluni casi, il trattamento di dati relativi al traffico a fini di sicurezza, ad esempio da parte delle società di sicurezza che forniscono servizi di sicurezza. Tale facoltà si basa sull'articolo 7, lettera f), che stabilisce che i responsabili del trattamento possono effettuare il trattamento di dati personali se ciò è «*necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata …*». La direttiva sulla tutela dei dati non specifica i casi in cui il trattamento di dati personali sarebbe tale da soddisfare detto requisito. Per contro, le decisioni sono adottate dai responsabili del trattamento, caso per caso, spesso con l'accordo delle autorità nazionali preposte alla protezione dei dati e di altre autorità.

79. Si dovrebbe esaminare l'interazione tra l'articolo 7 della direttiva sulla tutela dei dati e il proposto articolo 6, paragrafo 6 bis della direttiva e-privacy. Il proposto articolo 6, paragrafo 6 bis specifica le circostanze in cui i requisiti dell'articolo 7, lettera f) di cui sopra sarebbero soddisfatti. In effetti, autorizzando il trattamento di dati relativi al traffico al fine di contribuire a garantire la sicurezza delle reti e delle informazioni, l'articolo 6, paragrafo 6 bis autorizza tale trattamento per il perseguimento dell'interesse legittimo del responsabile del trattamento.

80. Come ulteriormente precisato in appresso, il GEPD ritiene che il proposto articolo 6, paragrafo 6 bis non sia né necessario né utile. In effetti, dal punto di vista giuridico, è in linea di principio superfluo stabilire se un particolare tipo di attività di trattamento di dati, nella fattispecie il trattamento di dati relativi al traffico a fini di sicurezza, soddisfi o meno i requisiti di cui all'articolo 7, lettera f) della direttiva sulla tutela dei dati, nel qual caso può essere necessario il consenso della persona interessata ai sensi dell'articolo 7, lettera a). Come sopra rilevato, tale valutazione è solitamente effettuata dai responsabili del trattamento, ossia le società, in sede di attuazione, in consultazione con le autorità preposte alla protezione dei dati e, ove necessario, dagli organi giurisdizionali. In generale, il

GEPD ritiene probabile che, in casi specifici, il legittimo trattamento dei dati relativi al traffico a fini di sicurezza, effettuato senza pregiudicare i diritti e le libertà fondamentali delle persone, soddisfi i requisiti di cui all'articolo 7, lettera f) della direttiva sulla tutela dei dati e possa pertanto essere effettuato. Inoltre, non esistono precedenti nell'ambito della direttiva sulla tutela dei dati e della direttiva e-privacy per operare una distinzione o riservare un trattamento speciale a determinati tipi di attività di trattamento di dati che soddisferebbero i requisiti di cui all'articolo 7, lettera f), e non è stata dimostrata la necessità di una siffatta eccezione. Per contro, come sopra rilevato, risulta che in numerosi casi questo tipo di attività sarebbe ampiamente in linea con il testo attuale. Pertanto una disposizione giuridica che confermi tale valutazione è in linea di principio superflua.

Formulazioni dell'articolo 6, paragrafo 6 bis elaborate dal PE, dal Consiglio e dalla Commissione

81. Come sopra precisato, è importante sottolineare che, benché superfluo, l'emendamento 181 quale adottato dal PE è stato nondimeno redatto, tenendo conto in certa misura dei principi relativi alla vita privata e alla protezione dei dati sanciti nella legislazione sulla protezione dei dati. L'emendamento 181 del PE avrebbe potuto tener maggiormente conto delle preoccupazioni concernenti la protezione dei dati e la vita privata, ad esempio inserendo l'espressione «in casi specifici» al fine di assicurare l'applicazione selettiva dell'articolo in questione o prevedendo un periodo specifico di conservazione.

82. L'emendamento 181 contiene alcuni elementi positivi. Esso conferma che il trattamento dovrebbe ottemperare ad ogni altro principio in materia di protezione dei dati applicabile al trattamento dei dati personali («*Senza pregiudizio per il rispetto delle disposizioni […] della direttiva 95/46/CE e […] della presente direttiva*»). Inoltre l'emendamento 181, benché autorizzi il trattamento dei dati relativi al traffico a fini di sicurezza, raggiunge un equilibrio tra gli interessi del soggetto che effettua il trattamento dei dati relativi al traffico e quelli delle persone i cui dati sono oggetto di trattamento, cosicché tale trattamento di dati può aver luogo soltanto se gli interessi del soggetto che effettua il trattamento dei dati non prevalgono sugli interessi per i diritti e le libertà fondamentali della persona interessata («*salvo ove su tali interessi prevalgano gli interessi per i diritti e le libertà fondamentali della persona interessata*»). Tale requisito è essenziale in quanto può permettere il trattamento dei dati relativi al traffico in casi specifici, ma non consentirebbe ad un soggetto di effettuare il trattamento dei dati relativi al traffico alla rinfusa.

83. La versione dell'emendamento riformulata dal Consiglio contiene elementi apprezzabili, quali l'inserimento dei termini «*strettamente necessaria*», che sottolineano il campo di applicazione limitato dell'articolo in questione. Tuttavia, la versione del Consiglio elimina le garanzie concernenti la protezione dei dati e la vita privata sopra menzionate. Sebbene in linea di principio si applichino le disposizioni generali in materia di protezione dei dati, a prescindere dalla presenza di un riferimento specifico in ogni singolo caso, la versione dell'articolo 6, paragrafo 6 bis formulata dal Consiglio può nondimeno essere interpretata come tale da conferire pieno potere discrezionale di effettuare il trattamento dei dati relativi al traffico senza essere soggetti alle garanzie concernenti la protezione dei dati e la vita privata che si applicano in caso di trattamento di dati relativi al traffico. Si potrebbe pertanto sostenere che i dati relativi al traffico possono essere raccolti, memorizzati e ulteriormente utilizzati senza dover ottemperare ai principi e agli obblighi specifici in materia di protezione dei dati che si applicano altrimenti ai soggetti responsabili, come il principio di qualità o l'obbligo di effettuare un trattamento in modo corretto e lecito e di garantire la riservatezza e la sicurezza dei dati. Inoltre, poiché l'articolo non contiene alcun riferimento ai principi applicabili in materia di protezione dei dati che impongono limiti temporali alla conservazione delle informazioni o a termini specifici, la versione del Consiglio può essere interpretata come tale da consentire la raccolta e il trattamento dei dati relativi al traffico a fini di sicurezza per un periodo indeterminato di tempo.

84. Inoltre, il Consiglio ha indebolito la protezione della vita privata in talune parti del testo estendendo potenzialmente la formulazione. Ad esempio, il riferimento al «*legittimo interesse del responsabile del trattamento*» è stato soppresso, suscitando dubbi in merito ai tipi di soggetti che potrebbero avvalersi di tale eccezione. È estremamente importante evitare di favorire la possibilità che qualsiasi utente o soggetto giuridico tragga vantaggio da tale modifica.

85. Le recenti esperienze nell'ambito del PE e del Consiglio dimostrano che è difficile definire mediante norme giuridiche la misura e le condizioni in cui il trattamento dei dati a fini di sicurezza può essere effettuato legalmente. È improbabile che qualsiasi articolo esistente o futuro elimini gli ovvi rischi di un'applicazione troppo estesa dell'eccezione per motivi diversi da quelli esclusivamente correlati alla sicurezza o da parte di soggetti che non dovrebbero poter beneficiare dell'eccezione. Ciò non significa che tale trattamento non possa aver luogo in ogni caso. Tuttavia, la possibilità di effettuare il trattamento e l'entità di quest'ultimo possono meglio essere valutate a livello di attuazione. I soggetti che intendono intraprendere tale trattamento dovrebbero discuterne la portata e le condizioni con le autorità preposte alla protezione dei dati ed eventualmente con il Gruppo dell'articolo 29. Alternativamente, la direttiva e-privacy potrebbe includere un articolo che autorizzi il trattamento dei dati relativi al traffico a fini di sicurezza, fatta salva l'esplicita autorizzazione delle autorità preposte alla protezione dei dati.

86. Tenendo conto, da un lato, dei rischi che l'articolo 6, paragrafo 6 bis presenta per il diritto fondamentale alla protezione dei dati e alla vita privata delle persone e, d'altro lato, del fatto che, come precisato nel presente parere, dal punto di vista giuridico tale articolo è superfluo, il GEPD è giunto alla conclusione che la migliore soluzione consisterebbe nella completa soppressione del proposto articolo 6, paragrafo 6 bis.

87. Nel caso in cui, in contrasto con la raccomandazione del GEPD, venga adottato un testo sulla falsariga dell'attuale versione dell'articolo 6, paragrafo 6 bis, detto testo dovrebbe comunque contenere le garanzie in materia di protezione dei dati sopra discusse. Esso dovrebbe altresì essere opportunamente integrato nell'attuale struttura dell'articolo 6, preferibilmente come nuovo paragrafo 2 bis.

V. **LA POSSIBILITÀ OFFERTA ALLE PERSONE GIURIDICHE DI PROMUOVERE AZIONI GIUDIZIARIE IN CASO DI VIOLAZIONE DELLA DIRETTIVA E-PRIVACY**

88. Il PE ha votato l'emendamento 133 che offre la possibilità ai fornitori di accesso a Internet ed altre persone giuridiche quali le associazioni di consumatori di promuovere un'azione giudiziaria contro le violazioni di una delle disposizioni della direttiva e-privacy ([19]). Purtroppo, né la Commissione né il Consiglio hanno accettato l'emendamento. Il GEPD ritiene tale emendamento molto positivo e ne raccomanda il mantenimento.

89. Per comprendere l'importanza di detto emendamento, occorre rendersi conto del fatto che, nel settore della protezione della vita privata e dei dati, il danno inflitto ad una persona considerata singolarmente non è generalmente sufficiente di per sé a giustificare la promozione di azioni giudiziarie da parte della persona interessata. Le persone di norma non adiscono un tribunale per conto proprio perché sono state vittime di spam o il loro nome è stato erroneamente inserito in un elenco. L'emendamento in questione consentirebbe alle associazioni di consumatori e ai sindacati che rappresentano gli interessi dei consumatori a livello collettivo di promuovere azioni giudiziarie per loro conto dinanzi a un organo giurisdizionale. Probabilmente, inoltre, una maggiore varietà di meccanismi di controllo favorirebbe un più ampio grado di osservanza e sarebbe pertanto nell'interesse di un'efficace applicazione delle disposizioni della direttiva e-privacy.

90. Esistono precedenti giuridici nei quadri normativi di alcuni Stati membri che prevedono già la possibilità di un'azione collettiva intesa a permettere ai consumatori o ai gruppi di interesse di chiedere un risarcimento alla parte che ha cagionato il danno.

91. Inoltre, il diritto della concorrenza di alcuni Stati membri ([20]) autorizza i consumatori, i gruppi di interesse (oltre al *concorrente leso*) ad adire le vie legali avverso il soggetto responsabile della violazione. La motivazione soggiacente a tale approccio consiste nel fatto che è probabile che le società che agiscono in violazione del diritto della concorrenza ne traggano vantaggio, poiché i consumatori che subiscono solo danni marginali sono di norma riluttanti ad adire le vie legali. Tale motivazione può applicarsi *mutatis mutandis* in materia di protezione dei dati e di vita privata.

92. Elemento più importante, come sopra menzionato, è il fatto che, autorizzando le persone giuridiche quali le associazioni di consumatori e i PPECS ad adire le vie legali, si favorisce la posizione dei consumatori e si promuove la generale osservanza della normativa sulla protezione dei dati. Se le società responsabili di violazioni incorrono in un rischio più elevato di essere oggetto di un'azione giudiziaria, è probabile che investano maggiormente nell'osservanza della normativa sulla protezione dei dati, con conseguente aumento a lungo termine del livello di protezione della vita privata e dei consumatori. Per tutti questi motivi il GEPD invita il PE e il Consiglio ad adottare una disposizione che consenta alle persone giuridiche di promuovere un'azione giudiziaria contro le violazioni di una delle disposizioni della direttiva e-privacy.

([19]) Articolo 13, paragrafo 6 della prima lettura del PE.

([20]) Si veda, ad esempio, il paragrafo 8 della legge tedesca contro la concorrenza sleale (LCSI).

VI. **CONCLUSIONI**

93. La posizione comune del Consiglio, la prima lettura del PE e la proposta modificata della Commissione contengono, in diversa misura, elementi positivi che servirebbero a rafforzare la protezione della vita privata e dei dati personali.

94. Tuttavia, il GEPD ritiene che vi sia un margine di miglioramento, in particolare per quanto riguarda la posizione comune del Consiglio che, purtroppo, non ha mantenuto alcuni degli emendamenti del PE intesi a contribuire ad assicurare un'adeguata protezione della vita privata e dei dati personali. Il GEPD esorta il PE e il Consiglio a ripristinare le garanzie in materia di vita privata incorporate nella prima lettura del PE.

95. Inoltre, il GEPD ritiene sia opportuno procedere ad una semplificazione di alcune disposizioni della direttiva. Ciò vale in particolare nel caso delle disposizioni in materia di violazioni di sicurezza, in quanto il GEPD ritiene che i vantaggi della notificazione di violazione si concretizzeranno in maniera ottimale se il quadro giuridico è stabilito correttamente sin dall'inizio. Infine, il GEPD ritiene sia opportuno migliorare e chiarire la formulazione di alcune disposizioni della direttiva.

96. Alla luce di quanto precede, il GEPD esorta il PE e il Consiglio ad intensificare gli sforzi al fine di migliorare e chiarire alcune disposizioni della direttiva e-privacy, ripristinando nel contempo gli emendamenti adottati dal PE in prima lettura e volti a garantire un livello appropriato di protezione della vita privata e dei dati. A tal fine, nei successivi punti 97, 98, 99 e 100 sono sintetizzate le problematiche in questione e sono formulate raccomandazioni e proposte redazionali. Il GEPD invita tutte le parti interessate a tenerne conto in quanto la direttiva e-privacy si avvia verso la fase dell'adozione definitiva.

Violazione di sicurezza

97. Il Parlamento europeo, la Commissione e il Consiglio hanno adottato approcci differenti per quanto riguarda la notificazione di violazioni di sicurezza. Le differenze tra i tre modelli riguardano segnatamente i soggetti contemplati dall'obbligo, il criterio o l'elemento di attivazione della notificazione, gli interessati autorizzati a ricevere la notificazione, ecc. È necessario che il PE e il Consiglio facciano tutto il possibile per produrre un quadro giuridico solido per quanto riguarda la violazione di sicurezza. A tal fine, il PE e il Consiglio dovrebbero:

— *mantenere* la definizione di violazione di sicurezza nei testi del PE, del Consiglio e della Commissione, in quanto essa è abbastanza generale per abbracciare la maggior parte delle pertinenti situazioni in cui la notificazione di violazioni di sicurezza potrebbe essere giustificata;

— per quanto riguarda la portata dei soggetti cui si deve applicare il proposto obbligo di notificazione, *includere* i fornitori di servizi della società dell'informazione. Anche i rivenditori in linea, le banche in linea e le farmacie in linea possono subire violazioni di sicurezza alla stessa stregua delle società di telecomunicazione, se non in misura maggiore. I cittadini si attenderanno di ricevere una notificazione non soltanto quando i fornitori dell'accesso a Internet subiscono violazioni di sicurezza ma in particolare quando ciò accade alle loro banche in linea e farmacie in linea.

— Per quanto riguarda l'attivazione della notificazione, il criterio previsto dalla proposta modificata «*ragionevolmente probabile che possa ledere*» è un criterio appropriato che assicura la funzionalità del sistema. Tuttavia, è importante far sì che il concetto di «ledere» sia sufficientemente ampio da contemplare tutte le pertinenti fattispecie di effetti negativi sulla vita privata o su altri interessi legittimi delle persone. Altrimenti, sarebbe preferibile introdurre un nuovo criterio in base al quale la notificazione sarebbe obbligatoria «*se vi è una probabilità ragionevole che la violazione produca effetti negativi per le persone*». L'approccio del Consiglio, secondo cui la violazione deve pregiudicare *gravemente* la vita privata di una persona, fornirebbe una protezione inadeguata ai singoli nella misura in cui tale criterio richiede che l'effetto sulla vita privata sia «grave». Ciò dà altresì adito a una valutazione soggettiva.

— Benché il coinvolgimento di un'autorità nel determinare se un soggetto interessato debba effettuare la notificazione alle persone abbia certamente effetti positivi, può risultare di difficile realizzazione e applicazione e può inoltre sottrarre risorse ad altre importanti priorità. Se le autorità non possono reagire con estrema rapidità, il GEPD teme che tale sistema possa perfino ridurre la protezione delle persone ed esercitare un'indebita pressione sulle autorità. Quindi, tutto considerato, il GEPD consiglia di *creare* un sistema in cui competa ai soggetti interessati valutare se essi debbano procedere alla notificazione.

— Al fine di consentire alle autorità di esercitare una supervisione sulle valutazioni effettuate dai soggetti contemplati in merito all'opportunità di effettuare una notificazione, il PE e il Consiglio dovrebbero *porre in atto* le garanzie seguenti:

  — *provvedere* affinché tali soggetti siano obbligati a notificare alle autorità tutte le violazioni che soddisfano il criterio prescritto;

  — *affidare* alle autorità un ruolo di supervisione, che consenta loro di essere selettive per poter essere efficaci. A tal fine, occorre aggiungere il seguente testo: «*Se l'abbonato o il singolo interessato non ha ancora ricevuto la notificazione, le autorità nazionali competenti, considerata la natura della violazione, possono chiedere ai PPECS o agli ISSP di provvedere alla notificazione*»;

  — *adottare* una nuova disposizione che prescriva ai soggetti interessati di mantenere piste di controllo interno dettagliate e globali. Ciò potrebbe essere conseguito con l'adozione del seguente testo: «*I PPECS e gli ISSP effettuano e conservano una registrazione completa e dettagliata di tutte le violazioni di sicurezza occorse, delle pertinenti informazioni tecniche ad esse correlate e delle misure adottate per porvi rimedio. I registri contengono altresì un riferimento a tutte le notificazioni effettuate agli abbonati o ai singoli interessati nonché alle autorità nazionali competenti, inclusi le relative date e il relativo contenuto. I registri sono prodotti all'autorità nazionale competente a sua richiesta*».

— Al fine di assicurare la coerenza nell'attuazione del quadro relativo alla violazione di sicurezza, il PE e il Consiglio dovrebbero *attribuire* alla Commissione la facoltà di adottare misure tecniche di attuazione, previa consultazione del GEPD, del Gruppo dell'articolo 29 e di altri pertinenti soggetti interessati.

— Per quanto riguarda i singoli cui deve essere effettuata la notificazione, si dovrebbero *utilizzare* i termini della Commissione o del PE «singoli interessati» o «utenti interessati» in quanto includono tutte le persone i cui dati personali sono stati compromessi.

Reti private accessibili al pubblico

98. I servizi di comunicazione sono spesso messi a disposizione del pubblico non attraverso reti pubbliche bensì attraverso reti gestite privatamente (ad es. punti Wi-Fi disponibili in alberghi e aeroporti), presumibilmente non contemplate dalla direttiva. Il PE ha adottato l'emendamento 121 (articolo 3) che amplia il campo di applicazione della direttiva per includervi le reti di comunicazione pubbliche e private nonché le reti private accessibili al pubblico. A tal fine, il PE e il Consiglio dovrebbero:

— *mantenere* la sostanza dell'emendamento 121, ma *riformularlo* facendo rientrare nel campo di applicazione della direttiva e-privacy «*il trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche o private accessibili al pubblico nella Comunità*». Le reti gestite a livello esclusivamente privato (a differenza delle reti private accessibili al pubblico) non sarebbero espressamente contemplate;

— *modificare* di conseguenza tutte le disposizioni operative per menzionare esplicitamente le reti private accessibili al pubblico oltre alle reti pubbliche;

— *includere* una modifica contenente la seguente definizione: «*"rete privata accessibile al pubblico": una rete gestita privatamente alla quale i membri del grande pubblico hanno di norma accesso senza restrizioni, a pagamento o gratuitamente o in connessione con altri servizi o offerte, fatta salva l'accettazione delle condizioni e modalità applicabili*». Ciò assicurerà una maggiore certezza del diritto per quanto riguarda i soggetti rientranti nel nuovo campo di applicazione;

— *adottare* un nuovo considerando, secondo cui la Commissione dovrebbe effettuare una consultazione pubblica sull'applicazione della direttiva e-privacy a tutte le reti private, con il contributo del GEPD, del Gruppo dell'articolo 29 e di altri pertinenti soggetti interessati. Occorrerebbe precisare che, a seguito della consultazione pubblica, la Commissione dovrebbe presentare proposte appropriate per estendere o limitare i tipi di soggetti che dovrebbero essere contemplati dalla direttiva e-privacy.

Trattamento dei dati relativi al traffico a fini di sicurezza

99. Il PE ha adottato in prima lettura l'emendamento 181 (articolo 6, paragrafo 6 bis), che autorizza il trattamento dei dati relativi al traffico a fini di sicurezza. Il Consiglio, nella sua posizione comune, ha adottato una nuova versione che affievolisce alcune della garanzie in materia di vita privata. Al riguardo, il GEPD raccomanda che il PE e il Consiglio:

— *respingano* tale articolo nella sua totalità in quanto superfluo e, se oggetto di abuso, tale da poter indebitamente minacciare la protezione dei dati e la vita privata delle persone;

— alternativamente, se dovesse essere adottata una qualche variante dell'articolo 6, paragrafo 6 bis, *incorporino* le garanzie in materia di protezione dei dati discusse nel presente parere (analoghe a quelle previste dall'emendamento del PE).

Azioni giudiziarie in caso di violazione della direttiva e-privacy

100. Il Parlamento ha adottato l'emendamento 133 (articolo 13, paragrafo 6) che attribuisce alle persone giuridiche la facoltà di promuovere un'azione giudiziaria contro le violazioni di una qualsiasi disposizione della direttiva. Purtroppo il Consiglio non ha accolto tale emendamento. Il Consiglio e il PE dovrebbero:

— *approvare* la disposizione che consente alle persone giuridiche, quali le associazioni di consumatori e di categoria, di promuovere azioni giudiziarie in caso di violazione di qualsiasi disposizione della direttiva (non solo in caso di violazione delle disposizioni in materia di spam, secondo l'attuale approccio della posizione comune e della proposta modificata). Una maggiore varietà di meccanismi di controllo favorirà un più ampio grado di osservanza e un'applicazione più efficace delle disposizioni della direttiva e-privacy nel suo insieme.

Raccogliere la sfida

101. In relazione a tutte le summenzionate questioni, il PE e il Consiglio devono raccogliere la sfida dell'elaborazione di norme e disposizioni adeguate, che siano attuabili e funzionali e rispettino il diritto alla protezione dei dati personali e della vita privata delle persone. Il GEPD auspica che le parti interessate facciano tutto il possibile per raccogliere tale sfida e spera che il presente parere contribuisca a tal fine.

Fatto a Bruxelles, il 9 gennaio 2009.

Peter HUSTINX

Garante europeo della protezione dei dati