I

(Risoluzioni, raccomandazioni e pareri)

PARERI

GARANTE EUROPEO DELLA PROTEZIONE DEI DATI

Parere del garante europeo della protezione dei dati in merito ai negoziati attualmente condotti dall'Unione europea per il raggiungimento di un accordo commerciale anticontraffazione (ACTA)

(2010/C 147/01)

IL GARANTE EUROPEO DELLA PROTEZIONE DEI DATI,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 16,

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/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 [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 [3], in particolare l'articolo 41,

HA ADOTTATO IL SEGUENTE PARERE:

I. INTRODUZIONE

1. L'Unione europea partecipa ai negoziati sulla formulazione di un accordo commerciale anticontraffazione (ACTA). Tali negoziati sono stati avviati nel 2007 da un gruppo iniziale di parti interessate e sono poi continuati con un gruppo più ampio di partecipanti; allo stato attuale essi includono Australia, Canada, Unione europea, Giappone, Corea, Messico, Marocco, Nuova Zelanda, Singapore, Svizzera e Stati Uniti. Nel 2008 la Commissione europea ha ricevuto mandato dal Consiglio per partecipare a questi negoziati.

2. Il Garante europeo della protezione dei dati (GEPD) riconosce che il commercio transfrontaliero di beni contraffatti e pirata rappresenta una crescente preoccupazione, che spesso coinvolge reti criminali organizzate e che richiede l'adozione di meccanismi appropriati di collaborazione a livello internazionale al fine di contrastare questa forma di criminalità.

3. Il GEPD ritiene che i negoziati condotti dall'Unione europea per il raggiungimento di un accordo multilaterale incentrato sul rispetto dei diritti di proprietà intellettuale sollevi questioni importanti, riguardanti l'impatto delle misure adottate per contrastare la contraffazione e la pirateria sui diritti fondamentali delle persone, in particolare sul diritto al rispetto della vita privata e alla protezione dei dati.

4. A questo proposito, il GEPD si rammarica in particolare per il fatto di non essere stato consultato dalla Commissione europea circa il contenuto di un simile accordo. Agendo di propria iniziativa, il GEPD ha quindi adottato l'attuale parere basato sull'articolo 41, paragrafo 2, del regolamento (CE) n. 45/2001 allo scopo di fornire un orientamento alla Commissione sugli aspetti relativi al rispetto della vita privata e alla protezione dei dati che dovrebbero essere presi in considerazione nei negoziati sull'ACTA.

II. SITUAZIONE ATTUALE E CONTENUTI PREVISTI DELL'ACTA

5. Il 7º ciclo di negoziati si è svolto in Messico dal 26 al 29 gennaio 2010, con l'intento di giungere a un accordo entro il 2010. Allo stato attuale non è però stata emessa alcuna bozza ufficiale d'accordo.

[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.

6. L'obiettivo dei negoziati è l'adozione di un nuovo accordo multilaterale volto a rafforzare il rispetto dei diritti di proprietà intellettuale e a contrastare la contraffazione e la pirateria. Se adottato, questo nuovo accordo creerebbe migliori norme internazionali sul comportamento da tenere per contrastare le violazioni su larga scala dei diritti di proprietà intellettuale. La DG Commercio della Commissione europea ha sottolineato in particolare che «l'obiettivo perseguito sono le azioni di contraffazione e di pirateria che influiscono in misura significativa sugli interessi commerciali, piuttosto che sulle attività dei normali cittadini» ([4]).

7. Quanto al contenuto dell'accordo, il *Riepilogo degli elementi principali oggetto di discussione* pubblicato dalla DG Commercio della Commissione europea nel novembre 2009 indica che l'obiettivo dell'ACTA di combattere la pirateria e la contraffazione sarà perseguito attraverso tre componenti principali: i) la cooperazione internazionale, ii) le prassi di applicazione della legge e iii) la definizione di un quadro giuridico per il rispetto dei diritti di proprietà intellettuale in alcune aree individuate, in particolare in ambiente digitale ([5]). Le misure previste si occuperanno segnatamente delle procedure giuridiche (quali ingiunzioni, misure provvisorie), del ruolo e delle responsabilità dei fornitori d'accesso a Internet (Internet Service Provider — ISP) nello scoraggiare la violazione del diritto d'autore tramite Internet e, inoltre, delle misure di cooperazione transfrontaliera volte a impedire l'attraversamento dei confini da parte dei beni. Le informazioni divulgate tratteggiano però soltanto le linee generali dell'accordo e non scendono nei dettagli di nessuna misura specifica e concreta.

8. Il GEPD osserva che, sebbene l'obiettivo attribuito all'ACTA sia quello di perseguire soltanto le violazioni su larga scala dei diritti di proprietà intellettuale, non si può escludere che le attività dei normali cittadini possano rientrare nel campo d'applicazione dell'ACTA, soprattutto vista l'adozione di misure esecutive in ambiente digitale. Il GEPD sottolinea che questo richiederà la definizione di garanzie appropriate per tutelare i diritti fondamentali delle persone. Inoltre, le leggi sulla protezione dei dati riguardano tutte le persone, anche quelle potenzialmente coinvolte in attività di contraffazione e di pirateria, e la lotta alle violazioni su larga scala interesserà certamente anche il trattamento dei dati personali.

9. A questo proposto, il GEPD incoraggia fortemente la Commissione europea ad avviare un dialogo pubblico e trasparente sull'ACTA, eventualmente per il tramite di una consultazione pubblica, in modo da aiutare a garantire che le misure previste siano conformi con i requisiti della normativa dell'Unione europea sul rispetto della vita privata e sulla protezione dei dati.

([4]) Cfr. http://trade.ec.europa.eu/doclib/docs/2009/november/tradoc_145271.pdf, pag. 2.

([5]) Cfr. la nota 2.

III. AMBITO DELLE OSSERVAZIONI DEL GEPD

10. Il GEPD si appella con forza all'Unione europea, in particolare alla Commissione europea che ha ricevuto il mandato di concludere l'accordo, affinché trovi un giusto equilibrio tra le esigenze di protezione dei diritti di proprietà intellettuale e i diritti delle persone al rispetto della vita privata e alla protezione dei dati.

11. Il GEPD sottolinea che il rispetto della vita privata e la protezione dei dati sono valori fondamentali dell'Unione europea, riconosciuti dall'articolo 8 della CEDU e dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea ([6]), che devono essere rispettati in tutte le politiche e le norme adottate dall'Unione europea ai sensi dell'articolo 16 del Trattato sul funzionamento dell'Unione europea (TFUE).

12. Il GEPD ribadisce inoltre che qualsiasi accordo raggiunto dall'Unione europea sull'ACTA dovrà soddisfare gli obblighi giuridici imposti all'Unione europea in materia di rispetto della vita privata e protezione dei dati ed enunciati in particolare nella direttiva 95/46/CE, nella direttiva 2002/58/CE ([7]) e nella giurisprudenza della Corte europea dei diritti dell'uomo ([8]) e della Corte di giustizia ([9]).

13. Il rispetto della vita privata e la protezione dei dati devono essere tenuti in considerazione già nella fase iniziale dei negoziati e non quando gli schemi e le procedure saranno stati definiti e concordati e sarà quindi troppo tardi per trovare soluzioni alternative e rispettose della vita privata.

14. Viste le scarse informazioni rese di pubblico dominio, il GEPD rileva di non essere in grado di fornire un'analisi delle disposizioni specifiche dell'ACTA. Nel presente parere, il GEPD si concentrerà pertanto sulla descrizione delle minacce al rispetto della vita privata e alla protezione dei dati che le misure concrete adottate nell'accordo, come è stato riferito, potrebbero porre nelle due aree seguenti: il rispetto dei diritti di proprietà intellettuale in ambiente digitale (capitolo IV) e i meccanismi di cooperazione internazionale (capitolo V).

([6]) Carta dei diritti fondamentali dell'Unione europea, GU C 303 del 14.12.2007, pag. 1.

([7]) Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), GU L 201 del 31.7.2002, pag. 37.

([8]) Che interpreta gli elementi principali e le condizioni enunciate nell'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU), adottata a Roma il 4 novembre 1950, in quanto applicabili a campi diversi. Cfr. in particolare la giurisprudenza menzionata in altri punti del presente parere.

([9]) Cfr. in particolare: causa C-275/06, *Productores de Música de España* (Promusicae), Racc. 2008, pag. I-271 e causa C-557/07, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, non ancora pubblicata.

IV. RISPETTO DEI DIRITTI DI PROPRIETÀ INTELLETTUALE IN AMBIENTE DIGITALE

IV.1. La necessità di analizzare le implicazioni delle «politiche di disconnessione da Internet dopo tre avvisi» sul rispetto della vita privata e sulla protezione dei dati

15. Secondo la Commissione europea, l'ACTA creerà un quadro giuridico volto a contrastare la pirateria in ambiente digitale ([10]). Tale quadro giuridico stabilirà le condizioni in base alle quali gli ISP e altri intermediari online ([11]) potranno essere ritenuti responsabili della circolazione di materiale lesivo del diritto d'autore all'interno dei loro sistemi. Questo quadro giuridico potrà inoltre stabilire i provvedimenti e le misure correttive da imporre agli utenti di Internet che caricheranno o scaricheranno materiale lesivo del diritto d'autore. Sebbene i dettagli di tale quadro giuridico non siano stati ufficialmente divulgati, le informazioni messe a disposizione da diversi canali suggeriscono che agli ISP potrebbe essere imposto l'obbligo di adottare le «politiche di disconnessione da Internet dopo tre avvisi», altrimenti denominate schemi di «risposta graduale». Tali schemi consentiranno ai beneficiari del diritto d'autore di controllare gli utenti di Internet e di individuare i presunti trasgressori del diritto d'autore. Dopo aver contattato gli ISP del presunto trasgressore, questi avvertiranno l'utente così identificato, informandolo che sarà disconnesso dall'accesso a Internet dopo che gli saranno stati trasmessi tre avvisi.

16. Contemporaneamente ai negoziati sull'ACTA, le politiche di disconnessione da Internet dopo tre avvisi sono in corso di attuazione in alcuni Stati membri, tra cui la Francia. Esse sono anche oggetto di discussione in vari forum dell'Unione europea, come il dialogo delle parti interessate sulle operazioni illegali di caricamento e scaricamento attualmente animato dalla DG MARKT, in combinazione con l'adozione della comunicazione della Commissione «Migliorare la tutela dei diritti di proprietà intellettuale nel mercato interno» ([12]). Discussioni su questo argomento hanno luogo anche in seno al Parlamento europeo nell'ambito del dibattito in corso su un progetto di risoluzione del Parlamento europeo sul miglioramento della tutela dei diritti di proprietà intellettuale nel mercato interno (denominato «relazione Gallo»).

17. Queste prassi sono altamente invasive della sfera privata delle persone e implicano il controllo generalizzato delle attività degli utenti di Internet, anche di quelle perfettamente legali. Esse interessano milioni di utenti di Internet rispettosi della legge, fra cui molti bambini e adolescenti, e sono affidate a soggetti privati, non alle autorità incaricate dell'applicazione della legge. Inoltre, al giorno d'oggi Internet riveste un ruolo centrale in quasi tutti gli aspetti della vita moderna, quindi gli effetti della disconnessione dell'accesso a Internet potrebbero essere enormi, escludendo le persone dal lavoro, dalla cultura, dalle applicazioni di governo elettronico ecc.

18. In questo contesto è importante valutare fino a che punto queste politiche sono conformi alla normativa dell'Unione europea sul rispetto della vita privata e sulla protezione dei dati e, più in particolare, se le politiche di disconnessione da Internet dopo tre avvisi costituiscono una misura necessaria per il rispetto dei diritti di proprietà intellettuale. Sarebbe inoltre opportuno verificare l'esistenza di metodi diversi e meno invasivi.

19. Non è ancora chiaro se le politiche di disconnessione da Internet dopo tre avvisi saranno inserite nell'ACTA. Tuttavia, queste politiche vengono prese in considerazione anche in altre aree e potrebbero avere un impatto enorme sulla protezione dei dati personali e sul rispetto della vita privata. Per questi motivi, il GEPD ritiene necessario affrontare l'argomento in questo parere. Prima di eseguire la verifica summenzionata, il GEPD descriverà brevemente il quadro giuridico applicabile per la protezione dei dati e il rispetto della vita privata.

20. È opportuno notare che le politiche di disconnessione da Internet dopo tre avvisi destano preoccupazioni non solo riguardo alla protezione dei dati e al rispetto della vita privata, ma anche riguardo ad altri valori, come il giusto processo e la libertà di parola. Tuttavia, questo parere si occuperà soltanto delle questioni legate alla protezione dei dati personali e al rispetto della vita privata delle persone.

IV.2. Le politiche di disconnessione da Internet dopo tre avvisi e l'applicazione del quadro giuridico dell'Unione europea sulla protezione dei dati e sul rispetto della vita privata

Come possono essere attuate le politiche di disconnessione da Internet dopo tre avvisi

21. In breve, con le politiche di disconnessione da Internet dopo tre avvisi i beneficiari del diritto d'autore che utilizzano mezzi tecnici automatizzati, eventualmente forniti da terzi, possono rilevare una presunta violazione del diritto d'autore controllando le attività degli utenti di Internet,

([10]) Cfr. la nota 2.

([11]) I diversi intermediari online possono essere definiti in base ai loro ruoli funzionali. Tuttavia, nel mondo reale gli intermediari assumono generalmente diverse di queste funzioni. Gli intermediari online comprendono: a) *fornitori d'accesso:* gli utenti si collegano alla rete tramite la connessione a un fornitore d'accesso; b) *operatori di rete:* forniscono i router, vale a dire le strutture tecniche necessarie per la trasmissione di dati; c) *host provider:* affittano lo spazio sul loro server, sul quale gli utenti o i fornitori di contenuti possono caricare i contenuti che desiderano. Gli utenti possono caricare e scaricare materiale su e da un servizio online, come una bacheca o una rete P2P.

([12]) Comunicazione della Commissione al Consiglio, al Parlamento europeo e al Comitato economico e sociale europeo «Migliorare la tutela dei diritti di proprietà intellettuale nel mercato interno», Bruxelles, 11 settembre 2009, COM(2009) 467 def.

per esempio sorvegliando forum e blog o spacciandosi per condivisori di file nelle reti paritetiche allo scopo di individuare i condivisori di file sospettati di scambiare materiale sottoposto al diritto d'autore ([13]).

22. Dopo aver individuato gli utenti di Internet presumibilmente coinvolti in una violazione del diritto d'autore attraverso i loro indirizzi di protocollo Internet (Internet Protocol — IP), i beneficiari del diritto d'autore invieranno gli indirizzi IP di tali utenti ai relativi fornitori d'accesso a Internet, che a loro volta avviseranno l'abbonato al quale appartiene l'indirizzo IP in merito al suo potenziale coinvolgimento in una violazione del diritto d'autore. Il ricevimento di un certo numero di avvisi da parte dell'ISP si tradurrà automaticamente nella cessazione o nella sospensione della connessione a Internet dell'abbonato da parte dell'ISP ([14]).

Il quadro giuridico applicabile dell'Unione europea sulla protezione dei dati e sul rispetto della vita privata

23. Le politiche di disconnessione da Internet dopo tre avvisi devono soddisfare i requisiti derivanti dal diritto al rispetto della vita privata, enunciati nell'articolo 8 della CEDU e nell'articolo 7 della Carta dei diritti fondamentali, nonché dal diritto alla protezione dei dati sancito dall'articolo 8 della Carta dei diritti fondamentali e dall'articolo 16 del TFUE ed esposto nella direttiva 95/46/CE e nella direttiva 2002/58/CE.

24. A parere del GEPD, il controllo del comportamento degli utenti di Internet, sommato alla raccolta dei loro indirizzi IP, costituisce un'interferenza nel loro diritto al rispetto della vita privata e della corrispondenza; sussiste pertanto un'interferenza nel loro diritto alla vita privata. Questo parere è in linea con la giurisprudenza della Corte europea dei diritti dell'uomo ([15]).

25. La materia è disciplinata dalla direttiva 95/46/CE ([16]), in quanto le politiche di disconnessione da Internet dopo tre avvisi riguardano il trattamento di indirizzi IP che — in ogni caso in base agli elementi di fatto — devono essere considerati dati personali. Gli indirizzi IP sono identificatori che appaiono come una stringa di numeri separati da punti, per esempio 122.41.123.45. Abbonandosi a un fornitore d'accesso a Internet, l'abbonato potrà accedere a Internet. Ogniqualvolta l'abbonato accederà a Internet, gli sarà attribuito un indirizzo IP attraverso il dispositivo utilizzato per l'accesso a Internet (per esempio un computer) ([17]).

26. Dedicandosi a una particolare attività, per esempio caricando materiale su Internet, l'utente potrà essere identificato da terzi attraverso l'indirizzo IP che ha utilizzato. Per esempio, se un utente che possiede l'indirizzo IP 122.41.123.45 ha caricato materiale presumibilmente lesivo del diritto d'autore su un servizio P2P alle 15.00 del 1º gennaio 2010, l'ISP sarà in grado di collegare questo indirizzo IP al nome dell'abbonato al quale ha assegnato tale indirizzo, accertandone così l'identità.

27. Se si considera la definizione dei dati personali contenuta nell'articolo 2 della direttiva 95/46/CE, «qualsiasi informazione concernente una persona fisica identificata o identificabile (persona interessata); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione» ([18]), non si può che concludere che gli indirizzi IP e le informazioni sulle attività collegate a questi indirizzi costituiscono dati personali in tutti i casi qui rilevanti. Infatti, un indirizzo IP serve come numero identificativo che consente di scoprire il nome dell'abbonato al quale è stato assegnato tale indirizzo IP. Inoltre, le informazioni raccolte a proposito dell'abbonato che possiede quell'indirizzo IP («ha caricato un determinato materiale sul sito web ZS alle 15.00 del 1º gennaio 2010») si riferiscono e attengono chiaramente alle attività di una persona identificabile (il possessore dell'indirizzo IP) e devono pertanto essere considerate dati personali.

([13]) La tecnologia P2P è un'applicazione software di calcolo distribuito che consente ai singoli computer di collegarsi e di comunicare direttamente con altri computer.

([14]) Esempi di sanzioni alternative includono la limitazione della funzionalità del collegamento a Internet, per esempio la velocità di connessione, il volume ecc.

([15]) Cfr. in particolare la sentenza della CEDU del 26 giugno 2006, *Weber e Saravia contro Germania* (dic.), n. 54934/00, paragrafo 77 e la sentenza della CEDU del 1º luglio 2008, *Liberty et al. contro Regno Unito*, n. 58243/00.

([16]) La Corte di giustizia adotta un approccio di larghe vedute all'applicabilità della direttiva 95/46/CE, le cui disposizioni devono essere interpretate alla luce dell'articolo 8 della CEDU. La Corte di giustizia ha stabilito nella sua sentenza del 20 maggio 2003, *Rundfunk*, cause congiunte C-465/00, C-138/01 e C-139/01, Racc. 2003, pag. I-4989, paragrafo 68, che «le disposizioni della direttiva 95/46/CE, poiché disciplinano il trattamento di dati personali che possono arrecare pregiudizio alle libertà fondamentali e, in particolare, al diritto alla vita privata, devono essere necessariamente interpretate alla luce dei diritti fondamentali, che secondo una costante giurisprudenza fanno parte integrante dei principi generali del diritto dei quali la Corte garantisce l'osservanza».

([17]) L'indirizzo IP che l'ISP attribuisce a una persona può essere sempre lo stesso ogni volta che questa persona naviga in Internet (nel qual caso si parla di indirizzi IP statici). Altri indirizzi IP sono invece dinamici, nel senso che il fornitore d'accesso a Internet attribuisce un indirizzo IP diverso ai suoi clienti ogniqualvolta questi si connettono a Internet. Ovviamente, l'ISP può collegare l'indirizzo IP ai dati dell'abbonato al quale ha assegnato l'indirizzo IP (statico o dinamico).

([18]) Il considerando 26 integra questa definizione: «considerando che i principi della tutela si devono applicare ad ogni informazione concernente una persona identificata o identificabile; che, per determinare se una persona è identificabile, è opportuno prendere in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona; che i principi della tutela non si applicano a dati resi anonimi in modo tale che la persona interessata non è più identificabile; …».

28. Questi pareri sono pienamente condivisi dal gruppo «Articolo 29» il quale, in un documento sulla protezione dei dati relativi ai diritti di proprietà intellettuale, ha affermato che gli indirizzi IP raccolti per far rispettare i diritti di proprietà intellettuale, e cioè per identificare gli utenti di Internet che hanno presumibilmente violato i diritti di proprietà intellettuale, sono dati personali nella misura in cui vengono utilizzati per far valere tali diritti nei confronti di una data persona ([19]).

29. La direttiva 2002/58/CE trova anch'essa applicazione, in quanto le politiche di disconnessione da Internet dopo tre avvisi comportano la raccolta di dati relativi al traffico e alle comunicazioni. La direttiva 2002/58/CE disciplina l'utilizzo di tali dati e sancisce il principio della riservatezza delle comunicazioni effettuate attraverso reti di comunicazione pubbliche e dei dati contenuti in tali comunicazioni.

IV.3. **Le politiche di disconnessione da Internet dopo tre avvisi costituiscono una misura necessaria?**

30. L'articolo 8 della CEDU enuncia i principi di necessità conformemente ai quali qualsiasi misura che violi il diritto al rispetto della vita privata delle persone è ammessa soltanto se costituisce una misura necessaria in una società democratica per lo scopo legittimo che essa persegue ([20]). Il principio di necessità ricorre anche negli articoli 7 e 13 della direttiva 95/46/CE e nell'articolo 15 della direttiva 2002/58/CE ([21]). Esso prevede un'analisi della proporzionalità della misura, che deve essere valutata sulla base della ponderazione degli interessi in causa, nel contesto della società democratica nel suo complesso ([22]), oltre a richiedere una valutazione dell'esistenza di misure alternative e meno invasive.

31. Pur riconoscendo l'importanza di far valere i diritti di proprietà intellettuale, il GEPD ritiene che una politica di disconnessione da Internet dopo tre avvisi come quella attualmente nota — che implica determinati elementi di applicazione generale — costituisca una misura sproporzionata e non possa pertanto essere considerata una misura necessaria. Il GEPD è altresì convinto dell'esistenza di soluzioni alternative e meno invasive o quanto meno del fatto che le politiche previste possano essere attuate in maniera meno invasiva o con un ambito più limitato. L'approccio dei tre avvisi pone inoltre problemi su un piano giuridico più dettagliato. Queste conclusioni saranno spiegate in prosieguo.

Le politiche dei tre avvisi sono sproporzionate

32. Il GEPD desidera sottolineare l'ampia portata delle misure imposte. A tal fine pone l'accento in particolare sui seguenti elementi:

i) il fatto che il controllo (nascosto) colpirebbe milioni di persone e *tutti* gli utenti, a prescindere dal fatto che siano o meno soggetti sospetti;

ii) il controllo comporterebbe la registrazione sistematica di dati, alcuni dei quali potrebbero dare adito a cause civili o addirittura penali nei confronti delle persone; inoltre, alcune delle informazioni raccolte sarebbero classificate come dati di natura delicata ai sensi dell'articolo 8 della direttiva 95/46/CE, dati questi che richiedono maggiori garanzie;

iii) il controllo genererà probabilmente molti casi di falsi positivi. La violazione del diritto d'autore non è questione facilmente risolvibile con un sì o con un no. Spesso i tribunali sono costretti a esaminare un numero considerevole di dettagli tecnici e giuridici distribuiti su decine e decine di pagine prima di poter stabilire se sia stata effettivamente perpetrata una violazione ([23]);

([19]) Gruppo «Articolo 29», documento di lavoro sulla protezione dei dati relativi ai diritti di proprietà intellettuale (WP 104), adottato il 18 gennaio 2005. Questo gruppo è stato istituito ai sensi dell'articolo 29 della direttiva 95/46/CE. Esso è un organo consultivo europeo indipendente sulla protezione dei dati e sul rispetto della vita privata. I suoi compiti sono descritti nell'articolo 30 della direttiva 95/46/CE e nell'articolo 15 della direttiva 2002/58/CE. Cfr. anche il parere 4/2007 del gruppo sulla nozione di dati personali (WP 136), adottato il 20 giugno 2007, in particolare a pag. 16.

([20]) L'articolo 8 della CEDU si riferisce espressamente al requisito per cui qualsiasi interferenza o restrizione deve essere «necessaria in una società democratica».

([21]) L'articolo 13 della direttiva 95/46/CE ammette una restrizione soltanto qualora costituisca «una misura necessaria alla salvaguardia: a) della sicurezza dello Stato; b) della difesa; c) della pubblica sicurezza; d) della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali o di violazioni della deontologia delle professioni regolamentate; e) di un rilevante interesse economico o finanziario di uno Stato membro o dell'Unione europea, anche in materia monetaria, di bilancio e tributaria; f) di un compito di controllo, ispezione o disciplina connesso, anche occasionalmente, con l'esercizio dei pubblici poteri nei casi di cui alle lettere c), d) ed e); g) della protezione della persona interessata o dei diritti e delle libertà altrui». L'articolo 15 della direttiva 2002/58/CE stabilisce che «tale restrizione costituisc[e], ai sensi dell'articolo 13, paragrafo 1, della direttiva 95/46/CE, una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica».

([22]) Cfr. anche la sentenza della CEDU del 2 agosto 1984, *Malone contro Regno Unito*, serie A n. 82, pag. 32, paragrafi 81 et seq. e la sentenza della CEDU del 4 dicembre 2008, *Marper contro Regno Unito* [GC], n. 30562/04 e 30566/04, paragrafi 101 et seq.

([23]) I tribunali possono dover valutare se il materiale è effettivamente protetto dal diritto d'autore, quali diritti sono stati violati, se l'utilizzo può essere considerato un caso di utilizzo corretto, la normativa applicabile, i danni ecc.

iv) gli *effetti* potenziali del controllo, che potrebbe causare la disconnessione dell'accesso a Internet. Ciò interferirebbe con il diritto alla libertà di espressione, alla libertà di informazione e di accesso alla cultura, alle applicazioni di e-government, ai mercati e alla posta elettronica, oltre a interferire in alcuni casi con le attività lavorative. In tale contesto è particolarmente importante rendersi conto che gli effetti saranno subiti non soltanto dal presunto trasgressore, ma anche da tutti i familiari che utilizzano la stessa connessione a Internet, ivi compresi i minori in età scolare che utilizzano Internet per le loro attività scolastiche;

v) il fatto che l'organismo incaricato di svolgere la valutazione e di prendere la relativa decisione sarà generalmente un organismo privato (vale a dire i beneficiari del diritto d'autore o l'ISP). Il GEPD ha già manifestato in un precedente parere le proprie preoccupazioni circa il controllo delle persone fisiche da parte del settore privato (per esempio, dagli ISP o dai beneficiari del diritto d'autore) in ambiti che ricadono in linea di principio sotto la competenza delle autorità incaricate dell'applicazione della legge ([24]).

33. Il GEPD non è convinto che i vantaggi prodotti dalle misure compenseranno l'impatto sui diritti fondamentali delle persone. La protezione del diritto d'autore è nell'interesse dei beneficiari e della società. Tuttavia, le limitazioni ai diritti fondamentali non sembrano affatto giustificate se si mettono a confronto la gravità dell'interferenza, vale a dire l'entità dell'intrusione nella vita privata messa in luce dagli elementi sopra descritti, e i vantaggi attesi sotto forma di prevenzione della violazione dei diritti di proprietà intellettuale, che riguarda perlopiù violazioni su piccola scala. Come indicato nelle conclusioni dell'avvocato generale Kokott in *Promusicae*: «Non è … certo che la condivisione degli archivi ad uso privato, soprattutto qualora abbia luogo senza scopo di lucro, possa recare un pregiudizio sufficientemente grave alla tutela dei diritti d'autore, tale da giustificare il ricorso a questa deroga. È infatti controverso in che misura la condivisione privata degli archivi possa recare un vero danno» ([25]).

34. In tale contesto è anche bene ricordare la reazione del Parlamento europeo agli «schemi dei tre avvisi» nell'ambito della revisione del pacchetto telecomunicazioni e, in particolare, l'emendamento 138 alla direttiva quadro ([26]). In tale emendamento è stato stabilito che qualsiasi restrizione ai diritti o libertà fondamentali può essere imposta soltanto se appropriata, proporzionata e necessaria nel contesto di una società democratica e la sua attuazione dev'essere oggetto di adeguate garanzie procedurali conformemente alla CEDU e ai principi generali del diritto comunitario, inclusi un'efficace tutela giurisdizionale e un giusto processo ([27]).

35. In quest'ottica, il GEPD sottolinea inoltre che qualsiasi limitazione dei diritti fondamentali sarà soggetta a un esame approfondito a livello nazionale e dell'Unione europea. In tale contesto è possibile fare un parallelo con la direttiva 2006/24/EC ([28]) riguardante la conservazione dei dati, che deroga al principio generale della protezione dei dati per quanto riguarda la loro cancellazione quando questi non sono più necessari al fine per il quale sono stati raccolti. Questa direttiva prevede che i dati relativi al traffico siano conservati allo scopo di perseguire i reati gravi. Si noti che la conservazione è ammessa soltanto per «reati gravi», che è limitata ai «dati relativi al traffico» che escludono in linea di principio le informazioni sul contenuto delle comunicazioni, e che sono richieste garanzie particolari. Nonostante ciò, sono stati sollevati dubbi circa la sua compatibilità con le norme sui diritti fondamentali; la Corte costituzionale rumena ha stabilito che la conservazione generalizzata è incompatibile con i diritti fondamentali ([29]), mentre presso la Corte costituzionale tedesca è in corso una causa a questo riguardo ([30]).

L'esistenza di mezzi diversi e meno invasivi

36. Le precedenti constatazioni sono confortate dall'esistenza di mezzi meno invasivi per l'ottenimento dello stesso scopo. Il GEPD insiste sul fatto che tali modelli meno invasivi debbano essere esaminati e sperimentati.

([24]) Parere del GEPD del 23 giugno 2008 sulla proposta di decisione che istituisce un programma comunitario pluriennale per la protezione dei minori che usano Internet e le altre tecnologie di comunicazione, GU C 2 del 7.1.2009, pag. 2.

([25]) Cfr. la causa di cui alla nota 8, punto 106.

([26]) Cfr. la direttiva 2009/140/CE del Parlamento europeo e del Consiglio del 25 novembre 2009, GU L 337 del 18.12.2009, pag. 37.

([27]) Il testo definitivo del cosiddetto emendamento 138 recita: «Articolo 1.3a. I provvedimenti adottati dagli Stati membri riguardanti l'accesso o l'uso di servizi e applicazioni attraverso reti di comunicazione elettronica, da parte degli utenti finali, devono rispettare i diritti e le libertà fondamentali delle persone fisiche, garantiti dalla convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e dai principi generali del diritto comunitario. Qualunque provvedimento di questo tipo riguardante l'accesso o l'uso di servizi e applicazioni attraverso reti di comunicazione elettronica, da parte degli utenti finali, che ostacolasse tali diritti o libertà fondamentali può essere imposto soltanto se appropriato, proporzionato e necessario nel contesto di una società democratica e la sua attuazione dev'essere oggetto di adeguate garanzie procedurali conformemente alla convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e ai principi generali del diritto comunitario, inclusi un'efficace tutela giurisdizionale e un giusto processo. Tali provvedimenti possono di conseguenza essere adottati soltanto nel rispetto del principio della presunzione d'innocenza e del diritto alla privacy. Dev'essere garantita una procedura preliminare equa ed imparziale, compresi il diritto della persona o delle persone interessate di essere ascoltate, fatta salva la necessità di presupposti e regimi procedurali appropriati in casi di urgenza debitamente accertata conformemente alla convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Dev'essere garantito il diritto ad un controllo giurisdizionale efficace e tempestivo.»

([28]) Direttiva 2006/24/CE del Parlamento europeo e del Consiglio del 15 marzo 2006, GU L 105 del 13.4.2006, pag. 54.

([29]) http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html

([30]) http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-124.html

37. In tale contesto, il GEPD ricorda che la direttiva modificata 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica (denominata «direttiva "diritti del cittadino"»), che costituisce parte integrante del pacchetto telecomunicazioni recentemente riformato, contiene alcune norme e procedure volte a limitare la violazione su piccola scala del diritto d'autore tra i consumatori ([31]). Tali procedure includono l'obbligo degli Stati membri di produrre informazioni standardizzate di pubblico interesse riguardanti vari argomenti, menzionando in particolare le violazioni del diritto d'autore e dei diritti connessi e le informazioni sulle conseguenze giuridiche di tali atti ([32]). Gli Stati membri possono quindi chiedere agli ISP di distribuire tale direttiva a tutti i loro clienti e di includerla nei loro contratti.

38. Il sistema ha lo scopo di informare e di dissuadere le persone dal divulgare informazioni sottoposte al diritto d'autore e dall'intraprendere attività illecite, evitando così il controllo dell'utilizzo di Internet e i relativi problemi legati al rispetto della vita privata e alla protezione dei dati. La direttiva «diritti del cittadino» dovrà essere attuata nel maggio 2011. Ne consegue che tali procedure non sono ancora state adottate e che non vi è ancora stato modo di testarne i benefici. Sembra pertanto prematuro trascurare i potenziali benefici di queste nuove procedure e abbracciare invece le «politiche di disconnessione dopo tre avvisi», che costituiscono una limitazione di gran lunga maggiore ai diritti fondamentali.

39. A integrazione di quanto precede, è opportuno ricordare che la direttiva 2004/48/CE del 28 aprile 2004 sul rispetto dei diritti di proprietà intellettuale prevede diversi strumenti per far valere i diritti di proprietà intellettuale presso i tribunali (discussi nei paragrafi 43 e seguenti) ([33]).

40. La direttiva sul rispetto dei diritti di proprietà intellettuale è stata recentemente recepita nella normativa degli Stati membri. Fino ad oggi non vi è stato tempo sufficiente per valutare se le sue disposizioni siano appropriate ai fini del rispetto dei diritti di proprietà intellettuale. Pertanto, l'esigenza di sostituire l'attuale sistema basato sui procedimenti giudiziari e non ancora testato è quanto meno dubbia. Quanto precede solleva l'inevitabile domanda sul perché le violazioni esistenti non possano essere adeguatamente punite con le sanzioni penali e civili a disposizione per la violazione del diritto d'autore. Di conseguenza, prima di proporre simili misure politiche, la Commissione dovrebbe fornire informazioni affidabili in grado di dimostrare l'incapacità dell'attuale quadro giuridico di produrre gli effetti desiderati.

41. Inoltre, non è chiaro se siano state fatte serie riflessioni circa la possibilità di adottare modelli economici alternativi che non implichino il controllo sistematico delle persone. Per esempio, dimostrando le perdite arrecate ai beneficiari del diritto d'autore dall'utilizzo P2P, i beneficiari e gli ISP potrebbero sperimentare abbonamenti differenziati per l'accesso a Internet in cui parte del prezzo di un abbonamento con accesso illimitato possa essere distribuita ai beneficiari del diritto d'autore.

La possibilità di svolgere un controllo mirato e meno invasivo

42. A prescindere dall'utilizzo di modelli completamente diversi, che dovrebbero essere esaminati e testati come sopra indicato, si potrebbe in ogni caso svolgere un controllo mirato e meno invasivo.

43. Il rispetto dei diritti di proprietà intellettuale può essere ottenuto anche attraverso il controllo di un numero solo limitato di persone sospettate di perpetrare una grave violazione del diritto d'autore. La direttiva sul rispetto dei diritti di proprietà intellettuale fornisce alcuni orientamenti in questo senso, illustrando i presupposti in base ai quali le autorità possono ordinare che i dati personali in possesso dei fornitori d'accesso a Internet siano divulgati allo scopo di far rispettare i diritti di proprietà intellettuale. L'articolo 8 stabilisce che l'autorità giudiziaria competente possa ordinare agli ISP di fornire le informazioni personali in loro possesso riguardanti i presunti autori di violazioni (per esempio, informazioni sull'origine e sulle reti di distribuzione di merci o di prestazione di servizi che violano un diritto di proprietà intellettuale) in risposta a una richiesta giustificata e proporzionata in caso di violazioni su *scala commerciale* ([34]).

44. Il criterio della «scala commerciale» è quindi decisivo. In base a tale criterio, il controllo può essere proporzionato nell'ambito di situazioni ad hoc, limitate e specificate in

([31]) Cfr. la direttiva 2009/136/CE del Parlamento europeo e del Consiglio del 25 novembre 2009, GU L 337 del 18.12.2009, pag. 11.

([32]) In particolare, l'articolo 21, paragrafo 4, della direttiva 2009/136/CE stabilisce che «[g]li Stati membri possono richiedere che le imprese di cui al paragrafo 3 diffondano, all'occorrenza, informazioni gratuite di pubblico interesse agli attuali e nuovi abbonati tramite gli stessi canali normalmente utilizzati dalle imprese per le loro comunicazioni con gli abbonati. In tal caso, dette informazioni sono fornite dalle competenti autorità pubbliche in forma standardizzata e riguardano fra l'altro: a) gli utilizzi più comuni dei servizi di comunicazione elettronica per attività illegali e per la diffusione di contenuti dannosi, in particolare quelli che possono attentare al rispetto degli altrui diritti e libertà. Rientrano in questa categoria le violazioni del diritto d'autore e dei diritti connessi e le informazioni sulle conseguenze giuridiche di tali atti (…).» Inoltre, l'articolo 20, paragrafo 1, recita: «Gli Stati membri possono inoltre richiedere che il contratto contenga ogni informazione che possa essere fornita a tal fine dalle competenti autorità pubbliche sull'utilizzo delle reti e servizi di comunicazione elettronica per attività illegali e per la diffusione di contenuti dannosi, e sugli strumenti di tutela dai rischi per la sicurezza personale, la vita privata e i dati personali di cui all'articolo 21, paragrafo 4, e relativi al servizio fornito.»

([33]) GU L 157 del 30.4.2004, pag. 45 (in prosieguo: direttiva sul rispetto dei diritti di proprietà intellettuale).

([34]) Ciò è ulteriormente confermato nel considerando 14 della direttiva sul rispetto dei diritti di proprietà intellettuale.

cui si abbiano validi motivi di sospettare un abuso del diritto d'autore su scala commerciale. Questo criterio può includere situazioni di evidente abuso del diritto d'autore da parte di soggetti privati allo scopo di ottenere benefici commerciali economici diretti o indiretti.

45. In pratica, per attuare il suddetto criterio, i beneficiari del diritto d'autore potrebbero svolgere un controllo mirato di taluni indirizzi IP al fine di verificare la portata della violazione del diritto d'autore. Ciò significa che i beneficiari sarebbero anche autorizzati a conservare per lo stesso scopo le relazioni che dimostrano l'esistenza della violazione. Tali informazioni dovrebbero essere usate soltanto dopo aver verificato la gravità della violazione, per esempio casi evidenti di gravi violazioni e di violazioni non gravi ma continuate, per un certo periodo di tempo, allo scopo di ottenere un vantaggio commerciale o un guadagno finanziario. Il requisito della continuità entro certi periodi di tempo viene sottolineato e approfondito in prosieguo nella trattazione sul principio di conservazione.

46. Ciò significa che, in questi casi, la raccolta di informazioni per dimostrare un presunto abuso di Internet potrebbe essere ritenuta proporzionata e necessaria allo scopo di preparare i procedimenti giudiziari, ivi comprese le azioni legali vere e proprie.

47. Quale ulteriore garanzia, il GEPD ritiene che le operazioni di trattamento dei dati finalizzate alla raccolta di questo genere di prove debbano essere preventivamente verificate e autorizzate dalle autorità nazionali preposte alla protezione dei dati. Il motivo risiede nel fatto che le operazioni di trattamento dei dati potrebbero comportare rischi specifici per i diritti e le libertà personali in virtù del loro stesso scopo, vale a dire intraprendere atti esecutivi che potrebbero rivelarsi penalmente perseguibili alla luce della natura delicata dei dati raccolti. Il fatto che il trattamento dei dati includa il controllo delle comunicazioni elettroniche è un ulteriore elemento a favore di una più attenta supervisione.

48. Il GEPD ritiene che la «scala commerciale» menzionata nella direttiva sul rispetto dei diritti di proprietà intellettuale sia un elemento molto appropriato per fissare i limiti del controllo allo scopo di rispettare il principio di proporzionalità. Inoltre, sembrano non esservi prove affidabili, in base ai criteri enunciati nella direttiva in questione, che l'azione legale nei confronti della violazione del diritto d'autore non sia possibile o efficace. Per esempio, le relazioni trasmesse dalla Germania — dove dal 2008, per effetto del recepimento della direttiva sul rispetto dei diritti di proprietà intellettuale, vi sono state circa 3 000 ordinanze dei tribunali a seguito delle quali gli ISP hanno divulgato ai tribunali informazioni su 300 000 abbonati — sembrano suggerire il contrario.

49. In breve, poiché la direttiva sul rispetto dei diritti di proprietà intellettuale è in vigore soltanto da due anni, è difficile capire per quale motivo i legislatori dovrebbero abbandonare i criteri contenuti in questa direttiva per passare a metodi più invasivi, quando l'Unione europea sta iniziando appena adesso a testare i metodi recentemente adottati. Per lo stesso motivo, è anche difficile comprendere la necessità di sostituire l'attuale sistema basato sui procedimenti giudiziari con altri tipi di misure (oltre a sollevare questioni legate al giusto processo, che non vengono affrontate in questa sede).

IV.4. **Conformità delle politiche di disconnessione da Internet dopo tre avvisi con le disposizioni più dettagliate sulla protezione dei dati**

50. Vi sono anche altre ragioni giuridiche più specifiche per le quali l'approccio dei tre avvisi risulta problematico dal punto di vista della protezione dei dati. Il GEPD desidera sottolineare la natura dubbia del motivo giuridico per il trattamento, previsto dalla direttiva 95/46/CE, e l'obbligo contenuto nella direttiva 2002/58/CE di cancellare i file di registro.

Motivo giuridico per il trattamento

51. Gli schemi dei tre avvisi includono il trattamento di dati personali, alcuni dei quali saranno usati per le procedure legali o amministrative volte a togliere l'accesso a Internet ai trasgressori recidivi. Da questo punto di vista, tali dati si classificano come dati delicati ai sensi dell'articolo 8 della direttiva 95/46/CE. L'articolo 8, paragrafo 5, stabilisce che «I trattamenti riguardanti i dati relativi alle infrazioni, alle condanne penali o alle misure di sicurezza possono essere effettuati solo sotto controllo dell'autorità pubblica, o se vengono fornite opportune garanzie specifiche, sulla base del diritto nazionale …».

52. In questo contesto è opportuno rimandare al documento del gruppo «Articolo 29» sopra menzionato, dove viene affrontata la questione del trattamento dei dati giudiziari ([35]). Il gruppo afferma che «Mentre ogni individuo ha ovviamente il diritto di trattare dati giudiziari nell'ambito dell'azione legale che lo concerne, il principio non è così ampio da consentire l'indagine approfondita, la raccolta e la centralizzazione di dati personali da parte di terzi, ivi compresa, in particolare, la ricerca sistematica su scala generale quali l'esplorazione di Internet (...); tali indagini rientrano nelle competenze delle autorità giudiziarie» ([36]). Mentre la raccolta di prove specifiche e mirate, soprattutto nei casi di gravi violazioni, può essere necessaria per stabilire ed esercitare un diritto legale, il GEPD condivide pienamente i pareri del gruppo «Articolo 29» circa l'assenza di legittimità delle indagini su vasta scala che implicano il trattamento di notevoli quantità di dati degli utenti di Internet.

53. La discussione sul principio di proporzionalità sopra descritta e il criterio della «scala commerciale» sono rilevanti per determinare in quali condizioni possa essere legittimata la raccolta di indirizzi IP e delle informazioni correlate.

([35]) Cfr. il paragrafo 28 del presente parere.
([36]) Sottolineatura aggiunta.

54. Gli ISP potrebbero tentare di legittimare il trattamento da parte dei beneficiari del diritto d'autore inserendo nei loro contratti con i clienti clausole che consentono il controllo dei loro dati e l'annullamento dei loro abbonamenti. Si potrebbe così ritenere che i clienti abbiano accettato di essere controllati sottoscrivendo simili contratti. Tuttavia, questa prassi solleva anzitutto la domanda basilare se le persone possano dare il proprio consenso agli ISP per un trattamento dei dati che non avverrà a cura dell'ISP, bensì di parti terze che non sono sottoposte all'«autorità» dell'ISP.

55. In secondo luogo si pone la questione della validità del consenso. L'articolo 2, paragrafo h, della direttiva 95/46/CE definisce il consenso come «qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento». Un aspetto importante è che, per essere valido, il consenso deve essere una manifestazione di volontà libera, specifica e informata della persona interessata, a prescindere dalle circostanze nelle quali viene concesso, secondo la definizione data nell'articolo 2, paragrafo h, della direttiva. Il GEPD ha seri dubbi circa il fatto che le persone cui viene chiesto il consenso al controllo delle loro attività su Internet avranno realmente la possibilità di operare una scelta, soprattutto perché l'alternativa sarebbe quella di non avere alcun accesso a Internet, il che potrebbe pregiudicare molti altri aspetti della loro esistenza.

56. In terzo luogo, è altamente discutibile se un simile controllo possa essere considerato *necessario* all'esecuzione di un contratto concluso con la persona interessata, come stabilito nell'articolo 7, paragrafo b, della direttiva 95/46/CE, in quanto il controllo non costituisce ovviamente l'oggetto del contratto concluso dalla persona interessata, ma soltanto un mezzo a disposizione dell'ISP per servire altri interessi.

Cancellazione dei file di registro

57. Ai sensi della direttiva 2002/58/CE e, più in particolare, del suo articolo 6, i dati relativi al traffico come gli indirizzi IP possono essere raccolti e memorizzati soltanto per ragioni direttamente correlate alla comunicazione stessa, ivi compresa la fatturazione, la gestione del traffico e la prevenzione della frode, dopodiché devono essere cancellati. Questo non osta gli obblighi previsti dalla direttiva riguardante la conservazione dei dati che, come già illustrato, prevede la conservazione dei dati relativi al traffico e la loro divulgazione alle forze di polizia e ai magistrati per aiutare l'indagine **soltanto su reati gravi** ([37]).

([37]) Cfr. il paragrafo 35 del presente parere.

58. Stando a quanto precede, gli ISP dovrebbero cancellare tutti i file di registro che rivelano le attività degli utenti di Internet e che non sono più necessari per gli scopi summenzionati. Visto che i file di registro non sono necessari per fini di fatturazione, sembrerebbe che le finalità di gestione del traffico degli ISP non richiedano più di tre o quattro settimane ([38]).

59. Ciò significa che, quando vengono contattati dai beneficiari del diritto d'autore (salvo qualora tale contatto avvenga entro il periodo limitato sopra indicato), gli ISP non dovrebbero più avere i file di registro che associano gli indirizzi IP ai relativi abbonati. La conservazione dei file di registro oltre tale periodo è ammessa soltanto per motivi giustificati rientranti nelle finalità previste dalla legge.

60. In pratica questo significa che, a meno che non siano trasmesse con la massima rapidità, le richieste indirizzate agli ISP dai beneficiari del diritto d'autore non potranno essere soddisfatte semplicemente perché l'ISP non disporrà più delle relative informazioni. Questo di per sé delimita il concetto di prassi di controllo accettabile, descritto nella precedente sezione.

Rischio di effetti di ricaduta

61. Il GEPD è inoltre preoccupato non solo per l'impatto che le politiche di disconnessione da Internet dopo tre avvisi possono avere sul rispetto della vita privata e sulla protezione dei dati, ma anche per i loro effetti di ricaduta. Se le politiche di disconnessione da Internet dopo tre avvisi dovessero essere autorizzate, esse potrebbero spianare la strada alla legittimazione di una sorveglianza ancora più stretta sulle attività degli utenti di Internet, in aree diverse e per scopi diversi.

62. Il GEPD esorta la Commissione a garantire che l'ACTA non prevarichi né contrasti il regime attualmente vigente nell'Unione europea con riguardo ai diritti di proprietà intellettuale, regime questo che rispetta i diritti e le libertà civili fondamentali come la protezione dei dati personali.

V. **PREOCCUPAZIONI RIGUARDANTI LA PROTEZIONE DEI DATI IN RAPPORTO AI MECCANISMI DI COOPERAZIONE INTERNAZIONALE**

63. Uno degli strumenti proposti dai partecipanti all'ACTA per risolvere la questione del rispetto dei diritti di proprietà intellettuale consiste nel promuovere la cooperazione

([38]) La gestione del traffico include l'analisi del traffico di rete dei computer al fine di ottimizzare o di garantire le prestazioni, una minore latenza e/o di aumentare la larghezza di banda utilizzabile.

internazionale attraverso una serie di misure volte a garantire il rispetto concreto dei diritti di proprietà intellettuale nelle giurisdizioni dei firmatari dell'ACTA.

64. Sulla scorta delle informazioni disponibili, si può prevedere che alcune delle misure pianificate per garantire il rispetto dei diritti di proprietà intellettuale riguarderanno la condivisione a livello internazionale di informazioni relative a presunte violazioni dei diritti di proprietà intellettuale tra le autorità pubbliche (quali le autorità doganali, le forze di polizia e gli organi di giustizia), come pure tra soggetti pubblici e privati (quali gli ISP e le associazioni dei beneficiari dei diritti di proprietà intellettuale). Questi trasferimenti di dati sollevano tutta una serie di questioni sul fronte della protezione dei dati.

V.1. **Gli scambi di dati sono considerati legittimi, necessari e proporzionati nel quadro dell'ACTA?**

65. Allo stato attuale del processo di negoziati, nel quale alcuni elementi concreti del trattamento dei dati rimangono indefiniti o sconosciuti, è impossibile verificare se il quadro di misure proposto sia conforme ai principi fondamentali di protezione dei dati e alla normativa dell'Unione europea sulla protezione dei dati.

66. C'è da chiedersi anzitutto se i trasferimenti di dati verso paesi terzi nel contesto dell'ACTA siano legittimi. Si potrebbe contestare l'opportunità di adottare misure a livello internazionale in questo campo, fintantoché tra gli Stati membri dell'Unione europea non esisterà alcun accordo sull'armonizzazione delle misure esecutive in ambiente digitale, né sui tipi di sanzioni penali applicabili ([39]).

67. In quest'ottica, pare che i principi di necessità e di proporzionalità dei trasferimenti di dati ai sensi dell'ACTA sarebbero più facilmente soddisfatti se l'accordo fosse espressamente limitato alla lotta contro le violazioni più gravi dei diritti di proprietà intellettuale, invece di prevedere trasferimenti di dati in blocco per qualsiasi sospetto di violazione dei diritti di proprietà intellettuale. A tal fine sarà necessario definire esattamente quali siano le «violazioni più gravi dei diritti di proprietà intellettuale» per le quali possano essere ammessi i trasferimenti di dati.

68. Occorre inoltre prestare particolare attenzione alle persone coinvolte negli scambi di dati e verificare se i dati saranno condivisi soltanto tra le autorità pubbliche o se implicheranno anche scambi tra soggetti privati e autorità pubbliche. Come illustrato in precedenza in questo parere, il coinvolgimento di soggetti privati in un'area che rientra in linea di principio sotto la competenza delle autorità incaricate dell'applicazione della legge desta tutta una serie di preoccupazioni ([40]). Le condizioni alle quali i soggetti privati saranno coinvolti nella raccolta e nello scambio con le autorità pubbliche di dati personali relativi a violazioni dei diritti di proprietà intellettuale dovrebbero essere rigorosamente limitate a circostanze specifiche e prevedere tutte le garanzie del caso.

V.2. **Normativa sulla protezione dei dati applicabile ai trasferimenti di dati nell'ambito dell'ACTA**

Regime generale per i trasferimenti di dati

69. Il quadro generale applicabile per la protezione dei dati nell'Unione europea è illustrato nella direttiva 95/46/CE, i cui articoli 25 e 26 definiscono il regime applicabile per i trasferimenti di dati verso paesi terzi. L'articolo 25 stabilisce che i trasferimenti debbano avvenire soltanto verso paesi che garantiscono un livello di protezione adeguato, in assenza del quale tali trasferimenti saranno vietati.

70. Il livello di adeguatezza garantito dai paesi terzi viene valutato caso per caso dalla Commissione europea, la quale ha emesso alcune decisioni in cui riconosce l'adeguatezza a una serie di paesi sulla base di un'analisi approfondita condotta dal gruppo «Articolo 29» ([41]).

71. IL GEPD osserva che la maggior parte dei partecipanti all'ACTA non rientra nell'elenco dei paesi che offrono un'adeguata protezione dei dati, stilato dalla Commissione: fatti salvi la Svizzera e, in circostanze specifiche, il Canada e gli Stati Uniti, tutti gli altri partecipanti all'ACTA non sono giudicati in grado di fornire un livello adeguato di protezione. Ciò significa che per trasferire dati dall'Unione europea a questi paesi deve essere soddisfatta almeno una delle condizioni dell'articolo 26, paragrafo 1, della direttiva 95/46/CE, oppure le parti del trasferimento di dati devono produrre garanzie adeguate in conformità con l'articolo 26, paragrafo 2, della direttiva.

Regime specifico per i trasferimenti di dati nell'ambito dell'applicazione del diritto penale

72. La direttiva 95/46/CE costituisce il principale strumento per la protezione dei dati nell'Unione europea, ma il suo campo d'applicazione è attualmente limitato, in quanto essa esclude espressamente le attività che riguardano, fra l'altro, le attività dello Stato in materia di diritto penale (articolo 3). Gli scambi di dati ai fini dell'applicazione del diritto penale ricadranno pertanto al di fuori del campo

([39]) Una proposta sulle sanzioni penali è attualmente oggetto di discussione in seno al Consiglio, COM(2006) 168 del 26 aprile 2006.

([40]) Cfr. i paragrafi 32 e 52 di questo parere. Cfr. anche il parere del GEPD dell'11 novembre 2008 sulla relazione finale del Gruppo di contatto ad alto livello UE-USA sulla condivisione delle informazioni e sulla tutela della vita privata e la protezione dei dati di carattere personale, GU C 128 del 6.6.2009, pag. 1.

([41]) Cfr. le decisioni in materia di adeguatezza emesse dalla Commissione europea nei confronti di Argentina, Canada, Svizzera, «Safe Harbor» per gli Stati Uniti e delle autorità statunitensi nel contesto PNR, Guernsey, Isola di Man e Jersey; disponibili all'indirizzo http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

di applicazione della direttiva 95/46/CE e saranno soggetti ai principi generali di protezione dei dati enunciati nella convenzione n. 108 del Consiglio d'Europa e nel suo protocollo aggiuntivo, cui hanno aderito tutti gli Stati membri dell'Unione europea ([42]). Troveranno inoltre applicazione le norme adottate dall'Unione europea in materia di cooperazione giudiziaria e di polizia in materia penale e riportate nella decisione quadro 2008/877/GAI del Consiglio ([43]).

73. Questi strumenti si fondano anche sul principio che debba essere garantito un livello adeguato di protezione dei dati nel paese terzo in cui i dati devono essere trasferiti. È prevista una serie di deroghe, in particolare laddove il paese terzo fornisca garanzie adeguate. Analogamente agli scambi di dati ai sensi della direttiva 95/46/CE, gli scambi di dati nell'ambito dell'applicazione del diritto penale richiederanno pertanto che siano prodotte garanzie adeguate tra le parti coinvolte nel trasferimento di dati, quale presupposto perché tale trasferimento possa avvenire.

Verso un nuovo regime per i trasferimenti di dati

74. È presumibile che nel prossimo futuro l'Unione europea adotterà nuove regole comuni per la protezione dei dati, applicabili a tutti i campi di attività dell'Unione europea, sulla base dell'articolo 16 del TFUE. Ciò significa che nel giro di qualche anno potrebbe esservi un quadro giuridico completo per la protezione dei dati a livello comunitario, fondato su norme coerenti per la protezione dei dati in tutti i campi di attività dell'Unione europea e in grado di imporre lo stesso livello di tutele e garanzie a tutte le attività di trattamento dei dati. Come illustrato da Viviane Reding ([44]), commissaria competente per la giustizia, i diritti fondamentali e la cittadinanza, questo nuovo quadro giuridico dovrebbe funzionare come un unico «strumento giuridico completo e moderno» per la protezione dei dati nell'Unione europea. Tale quadro giuridico è particolarmente auspicato, in quanto porterebbe maggiore chiarezza e coerenza riguardo alle norme applicabili nell'Unione europea in materia di protezione dei dati.

75. In un contesto internazionale, il GEPD rimanda anche alla risoluzione sulle norme internazionali per la protezione dei dati personali e il rispetto della vita privata, recentemente adottata dalle autorità preposte alla protezione dei dati, che rappresenta un primo passo verso la definizione di norme globali per la protezione dei dati ([45]). Le norme internazionali includono una serie di garanzie relative alla protezione dei dati, simili a quelle illustrate nella direttiva 95/46/CE e nella convenzione n. 108. Benché le norme internazionali non abbiano ancora valore vincolante, esse forniscono un utile orientamento circa i principi di protezione dei dati che possono essere volontariamente applicati dai paesi terzi per rendere il loro quadro giuridico compatibile con le norme dell'Unione europea. Il GEPD ritiene che, nel trattamento dei dati personali provenienti dall'Unione europea, i firmatari dell'ACTA dovrebbero anche tenere conto dei principi enunciati nelle norme internazionali.

V.3. **Necessità di adottare garanzie appropriate per proteggere i trasferimenti di dati dall'Unione europea verso paesi terzi**

Quale forma dovrebbero assumere le garanzie per proteggere efficacemente i trasferimenti di dati verso paesi terzi?

76. Qualora sia dimostrata la necessità di trasferire dati personali verso paesi terzi, il GEPD sottolinea che l'Unione europea dovrebbe negoziare con i paesi terzi destinatari — in aggiunta all'accordo ACTA stesso — strumenti specifici contenenti garanzie appropriate di protezione dei dati volte a disciplinare lo scambio di dati personali.

77. Le garanzie appropriate di protezione dei dati devono essere generalmente enunciate in un accordo vincolante tra l'Unione europea e il paese terzo destinatario, in virtù del quale la parte destinataria si impegna a rispettare la normativa comunitaria in materia di protezione dei dati e ad assicurare alle persone gli stessi diritti e le stesse misure correttive previste dalla normativa comunitaria. La necessità di un accordo vincolante è sancita dall'articolo 26, paragrafo 2, della direttiva 95/46/CE e dall'articolo 13, paragrafo 3, lettera b, della decisione quadro ed è inoltre supportata dalla prassi esistente dell'Unione europea di concludere accordi ad hoc per consentire trasferimenti di dati specifici verso paesi terzi ([46]).

78. Analogamente, in base ai progetti di norme internazionali, il destinatario può essere tenuto a garantire che provvederà al livello di protezione richiesto quale presupposto per il trasferimento. Queste garanzie possono anche assumere la forma di un impegno contrattuale.

Contenuto delle garanzie che devono essere prodotte dai firmatari dell'ACTA in rapporto ai trasferimenti di dati personali

79. Il GEPD sottolinea in particolare che gli scambi di informazioni a livello internazionale per fini di applicazione della legge sono particolarmente delicati dal punto di vista della protezione dei dati, in quanto un simile quadro giuridico

([42]) Convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981, e Consiglio d'Europa, protocollo addizionale alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati di carattere personale concernente le autorità di controllo ed i flussi transfrontalieri, Strasburgo, 8 novembre 2001.

([43]) Decisione quadro 2008/877/GAI del Consiglio del 27 novembre 2008 relativa alla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale, GU L 350 del 30.12.2008, pag. 60.

([44]) Cfr. le risposte al questionario del Parlamento europeo per la commissaria designata Viviane Reding, pag. 5, http://www.europarl.europa.eu/hearings/static/commissioners/answers/reding_replies_en.pdf

([45]) Risoluzione adottata a Madrid nel novembre 2009.

([46]) Per esempio, gli accordi dell'Europol e di Eurojust con gli Stati Uniti, l'accordo PNR, l'accordo Swift, l'accordo tra l'Unione europea e l'Australia sul trattamento e sul trasferimento dei dati del codice di prenotazione (*Passenger Name Record*, PNR) originari dell'Unione europea da parte dei vettori aerei all'amministrazione doganale australiana.

potrebbe legittimare trasferimenti massicci di dati in un ambito in cui l'impatto sulle persone è particolarmente forte e in cui si rende ancor più necessaria l'adozione di garanzie affidabili e rigorose.

80. Il GEPD spiega che le condizioni e garanzie specifiche possono essere definite soltanto caso per caso, alla luce di tutti i parametri relativi agli scambi di dati. A titolo di orientamento, il GEPD evidenzia comunque di seguito alcuni dei principi e delle garanzie che devono essere prodotte dai destinatari terzi quale presupposto per il trasferimento di dati:

— occorre verificare la giustificazione giuridica in base alla quale avvengono le attività di trattamento dei dati (e cioè: le operazioni di trattamento si basano su un obbligo giuridico, sul consenso delle persone interessate o su qualunque altra valida giustificazione?) e se i trasferimenti di dati rispettano lo scopo iniziale per il quale i dati sono stati raccolti. Non è ammesso alcun trasferimento al di fuori dello scopo specificato,

— la quantità e tipologia dei dati personali da scambiare devono essere chiaramente specificate e ridotte a quanto strettamente necessario per realizzare lo scopo del trasferimento. I dati personali raccolti e trasferiti possono includere segnatamente l'indirizzo IP degli utenti di Internet, la data e l'ora del sospetto reato e il tipo di reato. Il GEPD raccomanda di non associare i dati a nessuna persona specifica durante la fase d'indagine e ricorda che l'identificazione di un sospetto può avvenire soltanto nel rispetto della legge e sotto il controllo di un giudice. In quest'ottica, il GEPD chiarisce che i dati relativi a violazioni e sospette violazioni dei diritti di proprietà intellettuale sono una categoria speciale di dati, il cui trattamento è solitamente riservato alle autorità incaricate dell'applicazione della legge e richiede l'adozione di ulteriori garanzie. Le persone autorizzate a trattare i dati relativi alle violazioni e sospette violazioni dei diritti di proprietà intellettuale e le condizioni per il trattamento di tali dati devono quindi essere specificamente definite in conformità con la normativa esistente sulla protezione dei dati,

— le persone tra le quali i dati possono essere condivisi devono essere chiaramente specificate e gli inoltri ad altri destinatari devono essere vietati in linea di principio, salvo laddove tali inoltri siano necessari per un'indagine specifica. Questa limitazione riveste estrema importanza, in quanto i destinatari designati non devono condividere indebitamente le informazioni con destinatari non autorizzati,

— il GEPD ha motivo di ritenere che l'ACTA non prevederà soltanto la cooperazione tra autorità pubbliche, ma attribuirà mandati di applicazione della legge anche a organismi privati (come gli ISP, le associazioni dei beneficiari dei diritti d'autore ecc.). In quest'ultimo caso occorre valutare a fondo le condizioni e il grado di coinvolgimento degli organismi privati nell'applicazione dei diritti di proprietà intellettuale, nel senso che le misure dell'ACTA non dovrebbero conferire un diritto di fatto agli ISP e alle associazioni dei beneficiari dei diritti di proprietà intellettuale di controllare il comportamento degli utenti online. Inoltre, il trattamento dei dati personali da parte di organismi privati nell'ambito dell'applicazione della legge dovrebbe avvenire soltanto su una base giuridica appropriata. È altresì importante chiarire se gli organismi privati saranno tenuti a cooperare con le forze di polizia e in quale misura. Tale cooperazione dovrebbe in ogni caso essere limitata ai «reati gravi», che dovranno a loro volta essere precisamente definiti, in quanto non tutte le violazioni dei diritti di proprietà intellettuale sono da considerarsi reati gravi,

— il metodo usato per lo scambio di dati personali deve essere scelto accuratamente, specificando in particolare se tale scambio avverrà tramite un sistema «push» — per esempio, gli ISP e le associazioni dei beneficiari dei diritti di proprietà intellettuale trasferiranno sotto il proprio controllo una serie di dati a parti terze, quali le forze di polizia e le autorità incaricate dell'applicazione della legge, situate all'estero — o tramite un sistema «pull» — per esempio, le forze di polizia e le autorità incaricate dell'applicazione della legge avranno accesso diretto alle banche dati di parti private o alle banche dati centralizzate delle informazioni. Come già illustrato nell'ambito del PNR, un sistema «push» è l'unica opzione che risulta conforme ai principi di protezione dei dati dal punto di vista della protezione dei dati nell'Unione europea, in quanto consente al mittente nell'Unione europea, che è con tutta probabilità il responsabile del trattamento, di esercitare il proprio controllo sul trasferimento dei dati ([47]),

— occorre specificare il tempo di conservazione dei dati personali da parte dei destinatari, come pure lo scopo per il quale si rende necessaria tale conservazione. Questo periodo di conservazione deve essere proporzionato allo scopo da raggiungere, il che significa che i dati dovranno essere rimossi o cancellati quando non saranno più necessari per il raggiungimento di tale scopo,

— gli obblighi imposti ai responsabili del trattamento in paesi terzi devono essere chiaramente definiti. Dev'essere garantita l'esistenza di meccanismi di supervisione e/o di meccanismi attuabili di responsabilità, così da poter intraprendere ricorsi e comminare sanzioni efficaci nei confronti dei responsabili del trattamento

([47]) Cfr. il parere 4/2003 del gruppo «Articolo 29» sul livello di protezione garantito negli Stati Uniti per la trasmissione di dati relativi ai passeggeri, WP78, 13 giugno 2003.

in caso di trattamento indebito o di altri episodi rilevanti. Occorre inoltre mettere in atto meccanismi di ricorso, tali da consentire alle persone di sporgere denuncia presso un'autorità indipendente preposta alla protezione dei dati e di ottenere una risoluzione efficace dinanzi a un tribunale imparziale e indipendente ([48]),

— l'atto stipulato tra le parti deve specificare chiaramente i diritti delle persone interessate in relazione ai loro dati personali, ove tali dati siano trattati da un destinatario terzo, in modo da garantire che abbiano a disposizione mezzi efficaci per far valere i loro diritti in rapporto a un trattamento avvenuto all'estero,

— la trasparenza è inoltre fondamentale, e le parti che stipulano l'atto sulla protezione dei dati devono accordarsi su come informeranno le persone interessate in merito al trattamento in corso dei dati, nonché circa i loro diritti e le modalità previste per esercitarli.

VI. **CONCLUSIONI**

81. Il GEPD incoraggia fortemente la Commissione europea ad avviare un dialogo pubblico e trasparente sull'ACTA, eventualmente per il tramite di una consultazione pubblica, in modo da aiutare a garantire che le misure previste siano conformi ai requisiti della normativa dell'Unione europea sul rispetto della vita privata e sulla protezione dei dati.

82. In riferimento ai negoziati attualmente in corso sull'ACTA, il GEPD si appella alla Commissione europea affinché trovi un giusto equilibrio tra le esigenze di protezione dei diritti di proprietà intellettuale e il diritto al rispetto della vita privata e alla protezione dei dati. Il GEPD sottolinea l'importanza di dare la giusta considerazione al rispetto della vita privata e alla protezione dei dati già nella fase iniziale dei negoziati, prima che sia concordata qualsiasi misura, così da non dover cercare in un secondo momento soluzioni alternative e rispettose della vita privata.

83. È vero che la proprietà intellettuale è importante per la società e deve essere protetta, ma ciò non significa che debba essere posta al di sopra dei diritti fondamentali delle persone al rispetto della vita privata e alla protezione dei dati, né al di sopra di altri diritti quali la presunzione di innocenza, un'efficace tutela giurisdizionale e la libertà di espressione.

84. Nella misura in cui l'attuale bozza dell'ACTA include o quanto meno preme indirettamente a favore delle politiche di disconnessione da Internet dopo tre avvisi, l'ACTA limiterebbe profondamente i diritti e le libertà fondamentali dei cittadini europei, con particolare riguardo al rispetto della vita privata e alla protezione dei dati personali.

85. Il GEPD ritiene che le politiche di disconnessione da Internet dopo tre avvisi non siano necessarie al raggiungimento dello scopo di far rispettare i diritti di proprietà intellettuale. Il GEPD è convinto dell'esistenza di soluzioni alternative e meno invasive o quanto meno del fatto che le politiche previste possano essere attuate in maniera meno invasiva o con un ambito più limitato, segnatamente sotto forma di un controllo ad hoc mirato.

86. Le politiche di disconnessione da Internet dopo tre avvisi sono anche problematiche su un piano giuridico più dettagliato, in particolare perché il trattamento dei dati giudiziari, soprattutto da parte di organismi privati, deve essere fondato su una base giuridica appropriata. L'applicazione degli schemi dei tre avvisi può inoltre implicare la memorizzazione dei file di registro per periodi prolungati, il che sarebbe contrario alla normativa vigente.

87. Inoltre, nella misura in cui l'ACTA implica scambi di dati personali tra autorità e/o organismi privati situati nei paesi dei firmatari, il GEPD chiede all'Unione europea di adottare tutte le garanzie del caso. Tali garanzie dovrebbero essere applicate a tutti i trasferimenti di dati effettuati nell'ambito dell'ACTA (ai fini dell'applicazione del diritto civile, penale o delle normative in materia di tecnologie digitali) e dovrebbero essere conformi ai principi di protezione dei dati enunciati nella convenzione n. 108 e nella direttiva 95/46/CE. Il GEPD raccomanda che queste garanzie assumano la forma di accordi vincolanti tra i mittenti comunitari e i paesi terzi destinatari.

88. Il GEPD desidera inoltre essere consultato in merito alle misure da attuare in relazione ai trasferimenti di dati che avverranno in base all'ACTA, allo scopo di verificarne la proporzionalità e di accertarsi che garantiscano un livello adeguato di protezione dei dati.

Fatto a Bruxelles, addì 22 febbraio 2010.

Peter HUSTINX

Garante europeo della protezione dei dati

([48]) Cfr. il parere del Garante europeo della protezione dei dati sulla relazione finale del Gruppo di contatto ad alto livello UE-USA sulla condivisione delle informazioni e sulla tutela della vita privata e la protezione dei dati di carattere personale, 11.11.2008.