Sintesi del parere del Garante europeo della protezione dei dati sulla comunicazione congiunta della Commissione e dell'alto rappresentante dell'Unione europea per gli affari esteri e la politica di sicurezza «Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro» e sulla proposta di direttiva, presentata dalla Commissione, recante misure volte a garantire un livello comune elevato di sicurezza delle reti e dell'informazione nell'Unione

(Il testo completo del presente parere è reperibile in EN, FR e DE sul sito web del GEPD http://www.edps.europa.eu)

(2014/C 32/10)

1. **Introduzione**

1.1. *Consultazione del GEPD*

1. Il 7 febbraio 2013 la Commissione e l'alto rappresentante dell'Unione europea per gli affari esteri e la politica di sicurezza hanno adottato una comunicazione congiunta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni su una «Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro» ([1]) (in prosieguo «la comunicazione congiunta», «la strategia per la cibersicurezza» o «la strategia»).

2. Alla stessa data, la Commissione ha adottato una proposta di direttiva del Parlamento europeo e del Consiglio recante misure volte a garantire un livello comune elevato di sicurezza delle reti e dell'informazione nell'Unione ([2]) (in prosieguo «la proposta di direttiva» o «la proposta»). Tale proposta è stata trasmessa il giorno stesso al GEPD per consultazione.

3. Prima dell'adozione della comunicazione congiunta e della proposta, il GEPD ha avuto la possibilità di formulare osservazioni informali alla Commissione. Il GEPD si compiace del fatto che alcune di tali osservazioni siano state prese in considerazione nella comunicazione congiunta e nella proposta.

4. **Conclusioni**

74. Il GEPD accoglie con favore la presentazione da parte della Commissione e dell'alto rappresentante dell'Unione europea per gli affari esteri e la politica di sicurezza di una strategia per la cibersicurezza completa, integrata da una proposta di direttiva recante misure volte a garantire un livello comune elevato di sicurezza delle reti e dell'informazione nell'Unione. La strategia si aggiunge alle azioni politiche già sviluppate dall'UE in materia di sicurezza delle reti e dell'informazione.

75. Il GEPD accoglie positivamente il fatto che la strategia vada oltre l'approccio tradizionale che oppone la sicurezza alla vita privata prevedendo il riconoscimento esplicito della vita privata e della protezione dei dati come valori fondamentali che dovrebbero guidare la politica di cibersicurezza nell'Unione europea e a livello internazionale. Il GEPD rileva che la strategia per la cibersicurezza e la proposta di direttiva sulla sicurezza delle reti e dell'informazione possono svolgere un ruolo fondamentale nel contribuire a garantire la tutela dei diritti delle persone alla vita privata e alla protezione dei dati nell'ambiente online. Occorre al contempo garantire che esse non conducano a misure tali da costituire interferenze illecite con i diritti delle persone alla vita privata e alla protezione dei dati.

76. Il GEPD si compiace inoltre che la protezione dei dati sia citata in diverse parti della strategia e sia presa in considerazione nella proposta di direttiva sulla sicurezza delle reti e dell'informazione. Tuttavia, il GEPD si rammarica del fatto che la strategia e la proposta di direttiva non evidenzino in modo più adeguato il contributo alla sicurezza offerto dalla normativa esistente e futura sulla protezione dei dati e non garantiscano pienamente che gli obblighi derivanti dalla proposta di direttiva o altri elementi della strategia siano complementari con gli obblighi di protezione dei dati e non si sovrappongano o si contraddicano a vicenda.

77. Inoltre, il GEPD rileva che, non essendosi preso in considerazione e tenutosi pienamente conto di altre iniziative parallele della Commissione e delle procedure legislative in corso, come ad esempio la riforma della protezione dei dati e la proposta di regolamento in materia di identificazione elettronica e servizi fiduciari, la strategia per la cibersicurezza non fornisce una visione realmente globale e olistica della cibersicurezza nell'UE e rischia di perpetuare un approccio frammentato e parcellizzato. Il GEPD rileva

([1]) JOIN(2013) 1 final.
([2]) COM(2013) 48 final.

inoltre che la proposta di direttiva sulla sicurezza delle reti e dell'informazione non permette nemmeno di adottare un approccio globale alla sicurezza nell'UE e che l'obbligo fissato nella normativa sulla protezione dei dati costituisce probabilmente l'obbligo più completo in materia di reti e di sicurezza nel diritto dell'UE.

78. Il GEPD si rammarica inoltre del fatto che non sia considerato adeguatamente neanche l'importante ruolo delle autorità preposte alla protezione dei dati nell'attuazione e nel controllo dell'adempimento degli obblighi in materia di sicurezza e nel rafforzamento della cibersicurezza.

79. Per quanto riguarda la strategia per la cibersicurezza, il GEPD sottolinea quanto segue:

— una definizione chiara dei termini «ciberresilienza», «cibercrimine» e «ciberdifesa» è particolarmente importante, dal momento che questi termini sono utilizzati come giustificazione per alcune misure speciali che potrebbero causare interferenze con i diritti fondamentali, inclusi i diritti alla vita privata e alla protezione dei dati. Tuttavia, le definizioni di «cibercrimine» fornite nella strategia e nella convenzione sulla criminalità informatica restano molto ampie. Sarebbe opportuno disporre di una definizione chiara e *restrittiva* di «cibercrimine» piuttosto che di una definizione troppo ambiziosa,

— la normativa sulla protezione dei dati dovrebbe applicarsi a tutte le azioni della strategia ogniqualvolta queste riguardino misure che comportano il trattamento di dati personali. Sebbene la normativa sulla protezione dei dati non sia menzionata specificamente nelle sezioni relative al cibercrimine e alla ciberdifesa, il GEPD sottolinea che molte delle azioni previste in questi settori comporterebbero il trattamento di dati personali e rientrerebbero pertanto nell'ambito di applicazione della normativa vigente in materia di protezione dei dati. Il GEPD osserva inoltre che molte azioni consistono nella creazione di meccanismi di coordinamento, che richiederanno l'attuazione di adeguate garanzie di protezione dei dati per quanto riguarda le modalità di scambio dei dati personali,

— le autorità preposte alla protezione dei dati svolgono un ruolo importante nel contesto della cibersicurezza. Come custodi dei diritti delle persone alla vita privata e alla protezione dei dati, tali autorità sono attivamente impegnate nella protezione dei dati personali, sia offline sia online, e dovrebbero quindi essere opportunamente coinvolte nel loro compito di organismi di vigilanza in relazione all'attuazione delle misure che comportano il trattamento di dati personali (come ad esempio il lancio del progetto pilota dell'UE per la lotta contro *botnet* e *malware*). Anche altri attori nel campo della cibersicurezza dovrebbero cooperare con dette autorità nello svolgimento dei propri compiti, per esempio nello scambio di buone pratiche e di azioni di sensibilizzazione. Il GEPD e le autorità nazionali preposte alla protezione dei dati dovrebbero anche essere adeguatamente coinvolti nella conferenza di alto livello che sarà convocata nel 2014 per valutare i progressi compiuti nell'attuazione della strategia.

80. Per quanto riguarda la proposta di direttiva sulla sicurezza delle reti, il GEPD raccomanda al legislatore di:

— provvedere a una maggiore chiarezza e certezza nell'articolo 3, punto 8, sulla definizione degli operatori di mercato che rientrano nel campo di applicazione della proposta nonché costituire un elenco esaustivo comprendente tutte le parti interessate, al fine di garantire un approccio pienamente armonizzato e integrato alla sicurezza all'interno dell'Unione europea,

— chiarire all'articolo 1, paragrafo 2, lettera c), che la proposta di direttiva si applica alle istituzioni e agli organi dell'Unione europea, includendo un riferimento al regolamento (CE) n. 45/2001 all'articolo 1, paragrafo 5, della proposta,

— riconoscere un ruolo più trasversale per questa proposta in materia di sicurezza, prevedendo esplicitamente all'articolo 1 che essa debba applicarsi fatte salve le norme più dettagliate, già in essere o future, in aree specifiche (come quelle previste sui prestatori di servizi fiduciari nella proposta di regolamento in materia di identificazione elettronica),

— aggiungere un considerando per spiegare la necessità di integrare la protezione dei dati fin dalla progettazione e in modalità predefinita a partire dalla fase iniziale della progettazione dei meccanismi stabiliti nella proposta e nell'intero ciclo di vita di processi, procedure, organizzazioni, tecniche e infrastrutture interessate, tenendo conto della proposta di regolamento sulla protezione dei dati,

— chiarire le definizioni di «rete e sistema informativo» di cui all'articolo 3, punto 1 e di «incidente» di cui all'articolo 3, punto 4, e sostituire all'articolo 5, paragrafo 2, l'obbligo di istituire «un piano di valutazione dei rischi» con «la creazione e il mantenimento di un quadro di gestione dei rischi»,

— specificare nell'articolo 1, paragrafo 6, che il trattamento dei dati personali sarebbe giustificato ai sensi dell'articolo 7, lettera e), della direttiva 95/46/CE nella misura in cui ciò sia necessario per conseguire gli obiettivi d'interesse generale perseguiti dalla proposta di direttiva. Tuttavia, deve essere assicurato il rispetto dei principi di necessità e di proporzionalità, in modo che siano trattati solo i dati strettamente necessari al conseguimento dello scopo,

— elencare all'articolo 14 le circostanze in cui è richiesta una notifica nonché il contenuto e il formato di detta notifica, compresi i tipi di dati personali che devono essere notificati e se, e in quale misura, la notifica e i relativi documenti giustificativi debbano includere parti di dati personali interessate da uno specifico incidente di sicurezza (come ad esempio gli indirizzi IP). Si deve tener conto del fatto che le autorità competenti per la sicurezza delle reti e dell'informazione dovrebbero essere autorizzate a raccogliere ed elaborare dati personali nel quadro di un incidente di sicurezza solo quando strettamente necessario. Dovrebbero essere stabilite nella proposta appropriate misure di salvaguardia per garantire l'adeguata protezione dei dati trattati dalle autorità competenti per la sicurezza delle reti e dell'informazione,

— chiarire all'articolo 14 che le notifiche degli incidenti di cui all'articolo 14, paragrafo 2, dovrebbero applicarsi fatti salvi gli obblighi di notifica delle violazioni dei dati personali ai sensi della normativa applicabile in materia di protezione dei dati. Devono essere presentati nella proposta gli aspetti principali della procedura per la cooperazione delle autorità competenti per la sicurezza delle reti e dell'informazione con le autorità preposte alla protezione dei dati nei casi in cui l'incidente di sicurezza comporti una violazione di dati personali,

— modificare l'articolo 14, paragrafo 8, in modo che l'esclusione delle microimprese dal campo di applicazione della notifica non si applichi a quegli operatori che svolgono un ruolo cruciale nella prestazione di servizi della società dell'informazione, per esempio in considerazione della natura delle informazioni che elaborano (ad es. dati biometrici o dati sensibili),

— aggiungere nella proposta disposizioni che disciplinino l'ulteriore scambio di dati personali da parte delle autorità competenti per la sicurezza delle reti e dell'informazione con altri destinatari, al fine di garantire che i) i dati personali siano comunicati unicamente ai destinatari che devono procedere al trattamento per lo svolgimento dei propri compiti, conformemente a un'appropriata base giuridica; e ii) tali informazioni siano limitate a quanto necessario per l'assolvimento di detti compiti. Occorre altresì considerare il modo in cui le entità che forniscono i dati alla rete di condivisione delle informazioni garantiscono il rispetto del principio di limitazione delle finalità,

— specificare il limite di tempo per la conservazione dei dati personali per le finalità indicate nella proposta di direttiva, in particolare per quanto riguarda la conservazione da parte delle autorità competenti per la sicurezza delle reti e dell'informazione e all'interno dell'infrastruttura sicura della rete di cooperazione,

— ricordare alle autorità competenti per la sicurezza delle reti e dell'informazione il loro dovere di fornire informazioni appropriate agli interessati riguardo al trattamento dei dati personali, per esempio pubblicando sul proprio sito web la politica in materia di *privacy*,

— aggiungere una disposizione relativa al livello di sicurezza che deve essere rispettato dalle autorità competenti per la sicurezza delle reti e dell'informazione per quanto riguarda le informazioni raccolte, elaborate e scambiate. Dovrebbe essere specificamente incluso un riferimento ai requisiti di sicurezza di cui all'articolo 17 della direttiva 95/46/CE per quanto riguarda la protezione dei dati personali da parte delle autorità competenti per la sicurezza delle reti e dell'informazione,

— chiarire all'articolo 9, paragrafo 2, che i criteri per la partecipazione degli Stati membri al sistema sicuro di scambio di informazioni dovrebbero garantire un elevato livello di sicurezza e resilienza da parte di tutti i partecipanti ai sistemi di condivisione delle informazioni in tutte le fasi del trattamento. Tali criteri dovrebbero includere misure appropriate in materia di riservatezza e di sicurezza conformemente agli articoli 16 e 17 della direttiva 95/46/CE e agli articoli 21 e 22 del regolamento (CE) n. 45/2001. La Commissione dovrebbe essere espressamente vincolata da tali criteri per la sua partecipazione al sistema sicuro di scambio di informazioni in veste di responsabile del trattamento,

— aggiungere all'articolo 9 una descrizione dei ruoli e delle responsabilità della Commissione e degli Stati membri nella configurazione, gestione e manutenzione del sistema sicuro di scambio di informazioni e disporre che la progettazione del sistema sia effettuata in conformità dei principi di protezione dei dati fin dalla progettazione e in modalità predefinita nonché dei principi di sicurezza fin dalla progettazione,

— aggiungere all'articolo 13 che qualsiasi trasferimento di dati personali a destinatari situati in paesi al di fuori dell'UE dovrebbe avvenire in conformità degli articoli 25 e 26 della direttiva 95/46/CE e dell'articolo 9 del regolamento (CE) n. 45/2001.

Fatto a Bruxelles, il 14 giugno 2013

Peter HUSTINX

Garante europeo della protezione dei dati