Sintesi del parere del Garante europeo della protezione dei dati sulla comunicazione della Commissione europea al Consiglio e al Parlamento europeo sull'istituzione di un Centro europeo per la lotta alla criminalità informatica

(Il testo integrale del presente parere è reperibile in inglese, francese e tedesco sul sito web del GEPD http://www.edps.europa.eu)

(2012/C 336/05)

1. Introduzione

1.1. *Consultazione del GEPD*

1. Il 28 marzo 2012 la Commissione ha adottato una comunicazione dal titolo «Lotta alla criminalità nell'era digitale: istituzione di un Centro europeo per la lotta alla criminalità informatica» ([1]).

2. Il GEPD rileva che il Consiglio ha pubblicato le proprie conclusioni sull'istituzione di un Centro europeo per la lotta alla criminalità informatica il 7 e l'8 giugno 2012 ([2]). Il Consiglio approva gli obiettivi della comunicazione, appoggia l'istituzione del centro (denominato anche «EC3») all'interno di Europol nonché l'utilizzo delle attuali strutture al fine di agevolare l'interconnessione dei lavori su altri settori della lotta alla criminalità, conferma che l'EC3 deve fungere da punto di riferimento nella lotta alla criminalità informatica e che l'EC3 opererà in stretto contatto con agenzie e attori pertinenti a livello internazionale, e chiede alla Commissione, in consultazione con Europol, di precisare maggiormente la portata dei compiti specifici che permetteranno al centro di diventare operativo entro il 2013. Tuttavia, le conclusioni non fanno riferimento all'importanza dei diritti fondamentali e, in particolare, alla protezione dei dati nell'istituzione dell'EC3.

3. Prima dell'adozione della comunicazione della Commissione, il GEPD aveva avuto la possibilità di formulare osservazioni informali sul progetto di comunicazione. Nelle sue osservazioni informali, il GEPD aveva sottolineato che la protezione dei dati è un aspetto essenziale da tenere in considerazione nell'istituzione del Centro europeo per la lotta alla criminalità informatica (di seguito «EC3»). Purtroppo, la comunicazione non ha tenuto conto delle osservazioni formulate nella fase informale. Inoltre, le conclusioni del Consiglio chiedono di garantire che il centro diventi operativo già entro l'anno prossimo. Per questo motivo la protezione dei dati dovrà essere presa in considerazione nelle prossime misure che verranno adottate già a brevissimo termine.

4. Il presente parere tratta dell'importanza della protezione dei dati nell'istituzione dell'EC3 e fornisce suggerimenti specifici che potrebbero essere presi in considerazione nel corso dell'elaborazione del mandato dell'EC3 nonché nella revisione legislativa del quadro giuridico di Europol. Agendo di propria iniziativa, il GEPD ha quindi adottato il presente parere sulla base dell'articolo 41, paragrafo 2, del regolamento (CE) n. 45/2001.

1.2. *Ambito di applicazione della comunicazione*

5. Nella sua comunicazione, la Commissione segnala l'intenzione di istituire un Centro europeo per la lotta alla criminalità informatica quale priorità della strategia di sicurezza interna ([3]).

6. La comunicazione elenca in modo non esauriente diversi ambiti di criminalità informatica su cui dovrebbe concentrarsi l'EC3: reati informatici commessi da gruppi di criminalità organizzata, in particolare i reati informatici che permettono di realizzare ingenti profitti illegali quali la frode informatica, reati informatici che recano gravi danni alle vittime, quali lo sfruttamento sessuale dei minori on-line, e reati informatici con serie ripercussioni su sistemi critici delle tecnologie dell'informazione e della comunicazione (TIC) nell'Unione.

7. Per quanto riguarda il lavoro del centro, la comunicazione elenca quattro compiti principali ([4]):

— fungere da punto di riferimento europeo per le informazioni sulla criminalità informatica,

— mettere in comune le competenze europee in materia di criminalità informatica per aiutare gli Stati membri a rafforzare le loro capacità,

([1]) La criminalità informatica non è definita nella legislazione dell'UE.

([2]) Conclusioni del Consiglio sull'istituzione di un Centro europeo per la lotta alla criminalità informatica, 3172ª sessione del Consiglio «Giustizia e affari interni», Lussemburgo, 7 e 8 giugno 2012.

([3]) *La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura* [COM(2010) 673 def., del 22 novembre 2010]. Cfr. anche il parere del GEPD su questa comunicazione, formulato il 17 dicembre 2010 (GU C 101 dell'1.4.2011, pag. 6).

([4]) Comunicazione, pagg. 4-5.

— fornire sostegno agli Stati membri nelle indagini sulla criminalità informatica,

— diventare il portavoce degli investigatori europei sulla criminalità informatica a livello di autorità di contrasto e giudiziarie.

8. Le informazioni trattate dall'EC3 verranno raccolte dal *maggior numero possibile di fonti pubbliche, private o accessibili al pubblico*, arricchendo i dati di polizia disponibili, e *riguarderanno le attività di criminalità informatica, i metodi con cui tali attività vengono svolte e i loro presunti autori*. L'EC3 collaborerà inoltre direttamente con altre agenzie e organi europei, sia tramite la partecipazione di tali organismi al consiglio di direzione del centro che tramite la cooperazione operativa, se del caso.

9. La Commissione propone che l'EC3 sia l'interfaccia naturale delle attività di Interpol sulla criminalità informatica e delle altre unità internazionali di polizia preposte alla lotta contro la criminalità informatica. In collaborazione con Interpol e altri partner strategici nel mondo, l'EC3 dovrebbe inoltre sforzarsi di migliorare il coordinamento delle risposte nel quadro della lotta alla criminalità informatica.

10. In pratica, la Commissione propone di creare questo EC3 come parte di Europol. L'EC3 *farà parte di Europol* ([1]) e, di conseguenza, sarà assoggettato al regime giuridico di Europol ([2]).

11. Secondo la Commissione europea ([3]), le principali novità che l'EC3, nella formulazione proposta, apporterà alle attività attuali di Europol saranno: i) maggiori risorse per una maggiore efficienza nella raccolta di informazioni da varie fonti e ii) scambio di informazioni con partner esterni alla comunità delle autorità di contrasto (principalmente, partner del settore privato).

1.3. *Punto centrale del parere*

12. Nel presente parere il GEPD intende:

— chiedere alla Commissione di chiarire il campo di applicazione delle attività dell'EC3, nella misura in cui esse siano pertinenti per la protezione dei dati,

— valutare le attività previste nel contesto del quadro giuridico attuale di Europol, specialmente la loro compatibilità con il quadro,

— evidenziare gli aspetti pertinenti che il legislatore dovrebbe precisare più dettagliatamente nel contesto della futura revisione del regime giuridico di Europol al fine di garantire un maggiore livello di protezione dei dati.

13. Il parere è strutturato come segue. La parte 2.1 illustra perché la protezione dei dati è un elemento essenziale nella creazione dell'EC3. La parte 2.2 tratta la compatibilità tra gli obiettivi fissati nella comunicazione per l'EC3 e il mandato giuridico di Europol. La parte 2.3 verte sulla cooperazione con il settore privato e i partner internazionali.

3. **Conclusioni**

50. Il GEPD considera la lotta alla criminalità informatica un elemento fondamentale per il rafforzamento della sicurezza nello spazio digitale e per la creazione della fiducia necessaria. Il GEPD rileva che il rispetto dei regimi di protezione dei dati deve essere ritenuto parte integrante della lotta alla criminalità informatica e non un deterrente alla sua efficacia.

51. La comunicazione fa riferimento all'istituzione di un nuovo Centro europeo per la lotta alla criminalità informatica all'interno di Europol, benché un Centro per la lotta alla criminalità informatica di Europol esista già da diversi anni. Il GEPD vorrebbe vedere precisate più chiaramente le nuove funzioni e le attività che distingueranno il nuovo EC3 dall'attuale Centro per la lotta alla criminalità informatica di Europol.

([1]) Come raccomandato dallo studio di fattibilità pubblicato nel febbraio 2012, che valuta le differenti opzioni disponibili (status quo, istituzione presso Europol, proprietà/parte di Europol, centro virtuale), http://ec.europa.eu/home-affairs/doc_centre/crime/docs/20120311_final_report_feasibility_study_for_a_european_cybercrime_centre.pdf

([2]) Decisione del Consiglio, del 6 aprile 2009, che istituisce l'Ufficio europeo di polizia (Europol) (2009/371/GAI).

([3]) Comunicato stampa del 28 marzo, *Frequently Asked Questions: the new European Cybercrime Centre* Riferimento: MEMO/12/221. Data: 28 marzo 2012. http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/221

52. Il GEPD raccomanda di definire chiaramente le competenze dell'EC3 anziché limitarsi a esporle facendo riferimento al concetto di «criminalità informatica» incluso nell'attuale legislazione Europol. Inoltre, la definizione delle competenze e delle strategie di salvaguardia per la protezione dei dati dell'EC3 dovrà fare parte della revisione della legislazione Europol. Finché la nuova legislazione Europol non diventerà applicabile, il GEPD raccomanda che la Commissione enunci tali competenze e strategie di salvaguardia per la protezione dei dati nel mandato del centro. Tra queste potrebbero figurare:

— una definizione chiara dei compiti relativi al trattamento dei dati (in particolare, indagini e attività di sostegno operativo) che potrebbe svolgere il personale del centro, da solo o in collaborazione con squadre investigative comuni, e

— procedure chiare che da una parte garantiscano il rispetto dei diritti individuali (compreso il diritto alla protezione dei dati) e dall'altra forniscano garanzie che gli elementi di prova sono stati acquisiti legalmente e possono essere utilizzati dinanzi a un tribunale.

53. Il GEPD ritiene che gli scambi di dati personali dell'EC3 con il «maggior numero possibile di fonti pubbliche, private o accessibili al pubblico» implichino rischi specifici per la protezione dei dati poiché spesso comporteranno il trattamento di dati raccolti per fini commerciali e trasferimenti internazionali di dati. Questi rischi vengono affrontati dall'attuale decisione Europol, la quale stabilisce che, in generale, Europol non debba scambiare dati direttamente con il settore privato e effettuato possa farlo con determinate organizzazioni internazionali solo in circostanze molto specifiche.

54. In tale contesto, e considerata l'importanza di queste due attività per l'EC3, il GEPD raccomanda di fornire le opportune strategie di salvaguardia per la protezione dei dati conformemente alle disposizioni in vigore nella decisione Europol. Tali salvaguardie dovranno essere integrate nel mandato del centro che dovrà essere elaborato dalla squadra preposta alla realizzazione dell'EC3 (e successivamente nel quadro giuridico rivisto di Europol) e non dovranno in alcun modo tradursi in una minore protezione dei dati.

Fatto a Bruxelles, il 29 giugno 2012

Peter HUSTINX

Garante europeo della protezione dei dati