

PARERI

GARANTE EUROPEO DELLA PROTEZIONE DEI DATI

Parere del Garante europeo della protezione dei dati sulla decisione 2011/141/UE della Commissione che modifica la decisione 2007/76/CE della Commissione sul Sistema di cooperazione per la tutela dei consumatori («CPCS») e sulla raccomandazione 2011/136/UE della Commissione relativa alle linee guida per l'applicazione delle norme sulla protezione dei dati nell'ambito del CPCS

(2011/C 217/06)

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 gli articoli 7 e 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 richiesta di parere a norma dell'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001 concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati ⁽²⁾,

HA ADOTTATO IL SEGUENTE PARERE:

I. INTRODUZIONE

1. Il 1° marzo 2011 la Commissione europea ha adottato una nuova decisione che modifica la decisione 2007/76/CE sul CPCS («seconda modifica CPC») ⁽³⁾. Nella stessa data la Commissione ha adottato anche una raccomandazione relativa alle linee guida per l'applicazione delle norme sulla protezione dei dati nell'ambito del CPCS («linee guida CPC

⁽¹⁾ GU L 281 del 23.11.1995, pag. 31.

⁽²⁾ GU L 8 del 12.1.2001, pag. 1.

⁽³⁾ Decisione della Commissione, del 1° marzo 2011, che modifica la decisione 2007/76/CE recante attuazione del regolamento (CE) n. 2006/2004 del Parlamento europeo e del Consiglio sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa che tutela i consumatori per quanto concerne l'assistenza reciproca (2011/141/UE) (GU L 59 del 4.3.2011, pag. 63).

per la protezione dei dati») ⁽⁴⁾. Entrambi i documenti sono stati trasmessi al GEPD per la consultazione a norma dell'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001.

2. Il CPCS è un sistema informatico progettato e gestito dalla Commissione conformemente al regolamento (CE) n. 2006/2004 sulla cooperazione per la tutela dei consumatori («regolamento CPC»). Il CPCS facilita la cooperazione tra le «autorità competenti» degli Stati membri dell'UE e la Commissione nel settore della tutela dei consumatori per quanto concerne le violazioni di un insieme predefinito di direttive e regolamenti dell'UE. Per rientrare nella sfera di applicazione del regolamento CPC, le infrazioni devono avere natura transfrontaliera e danneggiare «gli interessi collettivi dei consumatori».
3. Nell'ambito della loro cooperazione, gli utenti del CPCS scambiano informazioni, tra cui dati personali. Tali dati personali possono riguardare direttori, dipendenti di un venditore o di un fornitore sospettati di un'infrazione, o gli stessi venditori o fornitori (in caso siano persone fisiche) e terzi quali consumatori o ricorrenti.
4. Il sistema è progettato per essere uno strumento di comunicazione sicuro tra le autorità competenti nonché per fungere da banca dati. Il CPCS viene utilizzato dalle autorità competenti al fine di richiedere informazioni, per contribuire all'esame di un caso ⁽⁵⁾ o per richiedere assistenza nell'esecuzione della normativa ⁽⁶⁾ («richieste di assistenza reciproca»). Inoltre, le autorità competenti possono anche inviare un messaggio di avvertimento («allarme») per informare altre autorità competenti e la Commissione di un'infrazione o di un sospetto d'infrazione ⁽⁷⁾. Il CPCS è altresì

⁽⁴⁾ Raccomandazione della Commissione, del 1° marzo 2011, relativa alle linee guida per l'applicazione delle norme sulla protezione dei dati nell'ambito del Sistema di cooperazione per la tutela dei consumatori (CPCS) (2011/136/UE) (GU L 57 del 2.3.2011, pag. 44).

⁽⁵⁾ Cfr. l'articolo 6 del regolamento CPC sullo «scambio di informazioni su richiesta».

⁽⁶⁾ Cfr. l'articolo 8 del regolamento CPC sulle «richieste di misure di esecuzione».

⁽⁷⁾ Cfr. l'articolo 7 del regolamento CPC sullo «scambio di informazioni in assenza di richiesta» (o «allarme» in breve).

dotato di ulteriori funzionalità, tra cui un sistema di notifica ⁽⁸⁾ e un forum per lo scambio di dati non connessi a casi specifici.

5. Nel presente parere il GEPD esamina una serie di questioni relative alla protezione dei dati riguardo al quadro giuridico del CPCS, concentrandosi principalmente sulla seconda modifica CPC adottata di recente. Il GEPD, inoltre, fa anche il punto sui progressi compiuti finora ed evidenzia selettivamente alcune questioni irrisolte nonché talune considerazioni per il futuro. Vengono inoltre formulate osservazioni su alcune disposizioni delle linee guida CPC per la protezione dei dati.
6. Contestualmente al presente parere, [adottato a norma dell'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001], il GEPD, in qualità di organo di controllo, formula anche un parere sul controllo preventivo (a norma dell'articolo 27 dello stesso regolamento) («parere sul controllo preventivo»). Il parere sul controllo preventivo fornisce una descrizione più dettagliata del CPCS e del trattamento dei dati personali contenuti in questo sistema. Nel parere sul controllo preventivo il GEPD formula raccomandazioni per l'adozione di misure specifiche a livello pratico, tecnico e organizzativo al fine di migliorare il rispetto dei principi di protezione dei dati nel CPCS. Considerando che le linee guida CPC per la protezione dei dati sono a loro volta strettamente connesse a queste misure specifiche, nel parere sul controllo preventivo vengono formulate osservazioni anche su determinate disposizioni delle linee guida.

II. QUADRO GIURIDICO DEL CPCS

7. Il GEPD si compiace che il CPCS si fonda su una solida base giuridica, nella fattispecie un regolamento adottato dal Consiglio e dal Parlamento. Inoltre, il GEPD rileva con soddisfazione che la base giuridica è stata integrata nel tempo al fine di fornire informazioni aggiuntive e affrontare le preoccupazioni riguardanti la protezione dei dati. In particolare, il GEPD si compiace del fatto che la decisione 2007/76/CE della Commissione, del 22 dicembre 2006, recante attuazione del regolamento CPC («decisione di attuazione CPC») sia stata adottata e in seguito ulteriormente modificata il 17 marzo 2008 e, successivamente, il 1° marzo 2011 con la seconda modifica CPC. Accoglie inoltre con favore l'adozione, da parte della Commissione, delle linee guida CPC per la protezione dei dati, specificamente incentrate su questioni concernenti la protezione dei dati.
8. Pur rammaricandosi di non essere stato consultato al momento dell'iniziale adozione del regolamento CPC e della decisione di attuazione CPC, il GEPD si compiace della consultazione da parte della Commissione in occasione dell'adozione delle due modifiche della decisione di attua-

zione CPC e delle linee guida CPC per la protezione dei dati. Il GEPD si compiace inoltre della precedente consultazione da parte della Commissione del gruppo di lavoro «articolo 29» sulla protezione dei dati («WP 29»), il quale il 21 settembre 2007 aveva emesso il proprio parere n. 6/2007 (WP 139). Infine, il GEPD accoglie con favore il riferimento a tali consultazioni formulato nei considerando delle linee guida CPC per la protezione dei dati.

9. Il GEPD rileva che i) la Commissione ha considerato attentamente sia le raccomandazioni fornite dal GEPD nell'ambito di scambi informali precedenti sia quelle espresse dal gruppo di lavoro «articolo 29» nel parere n. 6/2007 e che ii) a molte di queste raccomandazioni è seguito un successivo sviluppo del quadro legislativo del CPCS e/o a livello pratico, tecnico e organizzativo. Le osservazioni formulate dal GEPD nel presente parere e nel parere sul controllo preventivo devono essere considerate alla luce di queste premesse positive.

III. QUESTIONI RIGUARDANTI LA PROTEZIONE DEI DATI RIGUARDO ALLA SECONDA MODIFICA CPC

3.1. Conservazione dei dati personali nel CPCS

3.1.1. Introduzione

10. Come osservazione preliminare, il GEPD sottolinea che la questione delle chiusure dei casi e dei periodi di conservazione non è stata affrontata in maniera adeguata ed esauritiva nel regolamento CPC ⁽⁹⁾.
11. Di fatto, il regolamento CPC definisce solo due norme specifiche in materia di cancellazione dei dati e non ne fissa alcuna per quanto riguarda le chiusure dei casi ⁽¹⁰⁾. Innanzitutto stabilisce che, se un allarme «si rivela infondato», l'autorità competente deve ritirarlo e la Commissione deve cancellare immediatamente le informazioni dalla banca dati. In secondo luogo stabilisce che, quando un'autorità competente notifica, a norma dell'articolo 8, paragrafo 6, del regolamento CPC, che un'infrazione è cessata, i dati memorizzati devono essere soppressi cinque anni dopo la notifica.
12. Il regolamento CPC non precisa lo scopo del periodo di conservazione di cinque anni né specifica ulteriormente in quale modo e quando un allarme debba essere ritenuto «infondato». Analogamente, il regolamento CPC non definisce nemmeno i tempi di conservazione delle informazioni nella banca dati nei casi non contemplati dalle due norme specifiche appena menzionate (ad esempio, il regolamento non specifica per quanto tempo le richieste di assistenza

⁽⁸⁾ Cfr. gli articoli 7, paragrafo 2, e 8, paragrafo 6, del regolamento CPC.

⁽⁹⁾ Cfr. anche il parere n. 6/2007 del gruppo di lavoro «articolo 29» sulla protezione dei dati (menzionato nella parte II).

⁽¹⁰⁾ Cfr. l'articolo 10, paragrafo 2, del regolamento CPC.

reciproca vengono conservate nella banca dati qualora non abbiano dato luogo a misure di esecuzione efficaci che avrebbero potuto far cessare l'infrazione).

13. Il GEPD si compiace che la decisione di attuazione CPC modificata e le linee guida CPC per la protezione dei dati tentino di fornire ulteriori chiarimenti. Detto questo, il GEPD continua a nutrire riserve riguardo ad alcuni aspetti delle norme in materia di chiusura dei casi e di conservazione dei dati nel CPCS, illustrate di seguito nelle sezioni 3.1.2-3.1.4.

14. Il GEPD raccomanda di affrontare questi problemi in occasione della prossima revisione del quadro giuridico del CPCS, attraverso un'ulteriore modifica della decisione di attuazione CPC o, preferibilmente, prevedendo una modifica del regolamento CPC stesso.

15. Finché non sarà possibile attuare un intervento legislativo in tal senso, il GEPD raccomanda che i problemi concernenti i periodi di conservazione siano affrontati a livello pratico, tecnico e organizzativo e che siano anche illustrati chiaramente nella «Rete di cooperazione per la tutela dei consumatori: linee guida generali» di cui alla sezione 3.1.2.

3.1.2. Chiusure tempestive di casi

16. La seconda modifica CPC non fissa un termine ultimo entro il quale un caso di richiesta di assistenza reciproca (richiesta di informazioni o richiesta di esecuzione) deve essere chiuso.

17. Nel parere sul controllo preventivo il GEPD prende atto di una serie di misure concrete che la Commissione sta attualmente adottando per contribuire ad assicurare la chiusura tempestiva dei casi in sospeso.

18. Nel presente parere il GEPD raccomanda di fissare termini massimi per le richieste d'informazione e di esecuzione, le quali dovranno essere specificati in occasione della prossima revisione del quadro legislativo. Tali termini dovranno essere connessi al tipo di caso nonché all'attività effettiva. Al tempo stesso, le norme dovranno anche concedere una certa flessibilità alle autorità competenti affinché sia possibile estendere i casi per un valido motivo e per garantire che non siano chiusi prematuramente anche qualora la chiusura di un caso complesso richieda tempi più lunghi rispetto alla media.

19. A tal fine, il GEPD raccomanda di utilizzare come punto di partenza il documento intitolato «Rete di cooperazione per la tutela dei consumatori: linee guida generali», approvato

dal comitato CPC il 6 dicembre 2010. Il punto 2.7 delle linee guida generali, relativo a «fasi e termini in un caso CPC», illustra le controversie tipiche e stabilisce che, in media, le richieste d'informazioni devono essere gestite entro un periodo compreso tra uno e tre mesi. Secondo le linee guida generali, deve essere possibile gestire le richieste di esecuzione entro un periodo compreso in media tra i sei e i nove mesi (tranne che nel caso d'ingiunzioni o di ricorsi contro una decisione amministrativa, per cui un periodo di un anno o oltre è più realistico).

3.1.3. Allarmi

20. La seconda modifica CPC ha aggiunto un nuovo paragrafo al punto 2.2.2 dell'allegato alla decisione di attuazione CPC, il quale prevede che gli allarmi «fondati» siano ritirati dalla banca dati cinque anni dopo la loro emissione (quanto agli allarmi «infondati», le disposizioni esistenti prevedevano già il ritiro nel caso in cui «un allarme si rivela infondato»).

21. Per inquadrare questa nuova disposizione nel giusto contesto, il GEPD sottolinea che una delle sue preoccupazioni principali è assicurare che i dati personali non restino nella banca dati del CPCS più a lungo del necessario. Si tratta di una questione delicata, soprattutto per quanto riguarda gli allarmi (che hanno un numero di destinatari maggiore rispetto agli scambi bilaterali), in particolare quelli che si riferiscono ai sospetti d'infrazione. In pratica, in assenza di un termine preciso entro il quale l'allarme è mantenuto aperto, alcuni allarmi potrebbero restare in sospeso per un periodo indebitamente prolungato (fino a quando non ne sarà chiaramente dimostrata l'infondatezza). Tali azioni, basate su sospetti non confermati, comporterebbero rischi notevoli per il diritto fondamentale alla protezione dei dati, nonché per altri diritti fondamentali quali la presunzione di innocenza.

22. Di fronte a tale situazione, il GEPD si compiace che sia stato stabilito un periodo di conservazione per gli allarmi. Ciononostante, il GEPD ritiene che la Commissione non abbia fornito giustificazioni atte a dimostrare che un periodo di conservazione di cinque anni sarebbe proporzionato. Il GEPD raccomanda alla Commissione di svolgere una valutazione di proporzionalità e riesaminare la durata del periodo di conservazione per gli allarmi. In linea di principio, tutti gli allarmi notificati devono essere cancellati dalla banca dati molto prima, salvo che un allarme per segnalare un'infrazione o un sospetto d'infrazione non abbia dato luogo a una richiesta di assistenza reciproca e l'indagine transfrontaliera o l'azione di esecuzione non siano ancora in corso. La durata del periodo di conservazione deve essere tale da consentire a ciascuna autorità che riceve il messaggio di decidere se intende intraprendere indagini o azioni di esecuzione ulteriori e inviare una richiesta di assistenza reciproca tramite il CPCS; tuttavia, deve essere sufficientemente breve da ridurre al minimo il rischio di utilizzo improprio degli allarmi per la creazione di liste nere o l'estrazione di dati.

23. In quest'ottica il GEPD raccomanda alla Commissione di rivedere il quadro giuridico al fine di assicurare che gli allarmi siano cancellati al più tardi sei mesi dopo la loro trasmissione, salvo che non sia possibile giustificare un altro periodo di conservazione più appropriato.
24. Ciò dovrebbe contribuire ad assicurare in particolare che, in casi in cui il sospetto non sia stato confermato (o anche indagato ulteriormente), persone innocenti collegate al sospetto non siano mantenute in una «lista nera» e considerate «sospette» per un periodo indebitamente prolungato, il che contrasterebbe con l'articolo 6, lettera e), della direttiva 95/46/CE.
25. Questa limitazione è inoltre necessaria ad assicurare il principio della qualità dei dati [cfr. l'articolo 6, lettera d), della direttiva 95/46/CE] nonché altri importanti principi giuridici e non solo potrebbe tradursi in un livello più adeguato di protezione delle persone, ma, al tempo stesso, dovrebbe anche permettere ai funzionari incaricati dell'esecuzione di concentrarsi più efficacemente sui casi pertinenti.
- 3.1.4. *Periodo di conservazione per le richieste di assistenza reciproca chiuse*
26. Con la seconda modifica CPC è stato aggiunto un nuovo paragrafo al punto 2.15 dell'allegato alla decisione di attuazione CPC al fine di stabilire che «[t]utte le altre informazioni riguardanti richieste di assistenza reciproca di cui all'articolo 6 (del regolamento CPC) sono cancellate dalla banca dati cinque anni dopo la chiusura del caso».
27. Letto in combinato disposto con il testo esistente, il punto 2.15 rivisto stabilisce che tutti gli scambi d'informazioni di cui all'articolo 6 vengano conservati per cinque anni dopo la chiusura del caso escluso laddove:
- i dati errati siano stati cancellati,
 - lo scambio di informazioni non abbia dato origine ad un allarme o ad una richiesta di esecuzione; o
 - sia stato accertato che non ha avuto luogo alcuna infrazione ai sensi del regolamento CPC.
28. Di fatto, come spiegato nel parere sul controllo preventivo, il periodo di conservazione «standard» applicato nel CPCs dopo la chiusura di un caso (salvo specifiche eccezioni) sembra essere di cinque anni sia per le richieste d'informazioni che per le richieste di esecuzione.
29. Il testo della decisione di attuazione CPC quale modificato dalla seconda modifica CPC non sembra essere pienamente coerente con il regolamento CPC. In particolare, l'articolo 10, paragrafo 2, del regolamento CPC opera una distinzione tra, da un lato, le informazioni scambiate che danno origine a un'efficace applicazione delle normative (ad esempio i casi in cui l'infrazione sia cessata a seguito delle misure di esecuzione attuate) e, dall'altro, le informazioni da cui non è scaturita un'applicazione efficace. Per le prime è previsto un periodo di conservazione di cinque anni dopo la chiusura del caso, mentre per le seconde non sono illustrate disposizioni specifiche (fuorché il ritiro e la soppressione degli allarmi infondati).
30. In altre parole, il regolamento CPC prescrive un periodo di conservazione di cinque anni dopo la chiusura del caso solo a condizione che siano state adottate misure di esecuzione e che queste abbiano determinato la cessazione dell'infrazione.
31. Benché il GEPD nutra alcune riserve in merito allo scopo e alla proporzionalità della conservazione di tutti i dati per cinque anni dopo la chiusura del caso (si vedano le osservazioni formulate al riguardo nella sezione 3.1.4), la distinzione tra i casi che si sono conclusi con un'efficace applicazione delle normative e quelli che invece non hanno avuto buon esito in tal senso ha una certa logica dal punto di vista della protezione dei dati. In particolare, la conservazione dei dati riguardanti semplici sospetti per un periodo prolungato presenta un maggiore potenziale di imprecisione e rischia altresì di violare altri principi giuridici importanti. In linea generale, dunque, si può affermare che è più probabile che la conservazione di tali dati per un periodo di tempo prolungato determini problemi in materia di protezione dei dati rispetto alla conservazione di dati relativi a infrazioni effettive, che sono state adeguatamente dimostrate e hanno dato luogo a misure di esecuzione.
32. Diversamente dal regolamento CPC, la decisione di attuazione CPC modificata sembra consentire, almeno in certi casi, l'applicazione del periodo di conservazione di cinque anni anche alle informazioni che non hanno dato luogo a misure di esecuzione efficaci.
33. Ad esempio, secondo la decisione di attuazione CPC, una richiesta di informazioni che ha dato origine ad un allarme senza però aver dato luogo a misure di esecuzione efficaci sembra rimanere nel sistema per cinque anni dopo la «chiusura del caso».

34. Il regolamento CPC e la decisione di attuazione CPC sembrano pertanto seguire un approccio leggermente diverso l'uno dall'altra. La decisione di attuazione CPC, pur rispecchiando in certa misura le disposizioni del regolamento CPC, introduce anche norme aggiuntive importanti in materia di conservazione. Benché la chiarificazione delle norme sia di per sé un elemento positivo, il GEPD contesta la legittimità di istituire periodi di conservazione più lunghi nei casi in cui il regolamento CPC non contenga già disposizioni in tal senso. Tale misura limiterebbe ulteriormente il diritto fondamentale alla protezione dei dati nell'applicazione della normativa, in contrasto con il regolamento CPC e le norme applicabili in materia di protezione dei dati.

35. In base alle precedenti considerazioni, il GEPD raccomanda alla Commissione di rivedere il quadro giuridico e riconsiderare se il periodo di conservazione di cinque anni deve essere applicato a tutti gli altri casi oltre a quelli che hanno dato luogo a un'efficace applicazione delle normative come specificato nel regolamento CPC.

36. Il GEPD si compiace inoltre che le linee guida CPC per la protezione dei dati intendano precisare lo scopo del periodo di conservazione dei dati dopo la chiusura di un caso, una questione importante che non è stata affrontata né nel regolamento CPC né nella seconda modifica CPC. In particolare, le linee guida CPC per la protezione dei dati stabiliscono che «durante il periodo di conservazione, gli agenti che lavorano per un'autorità competente a cui un dato caso è stato inizialmente affidato possono consultare la pratica in questione per verificare i legami con eventuali infrazioni ripetute, in modo da migliorare e rendere più efficiente l'azione di contrasto»⁽¹¹⁾.

37. Tuttavia, pur accogliendo con favore questo chiarimento, in assenza di ulteriori giustificazioni della necessità di tale accesso, il GEPD non è convinto della proporzionalità e della sufficienza di questo scopo per giustificare il periodo di conservazione di cinque anni. Il GEPD raccomanda pertanto alla Commissione di:

- precisare ulteriormente lo scopo del periodo di conservazione di cinque anni,
- valutare se un periodo di conservazione più breve consentirebbe di raggiungere gli stessi obiettivi; e

⁽¹¹⁾ Cfr. la sezione 8 delle linee guida, «Altre indicazioni; Perché il periodo di conservazione dei dati è stato fissato in 5 anni?» Le linee guida CPC per la protezione dei dati aggiungono inoltre che «lo scopo del periodo di conservazione è facilitare la cooperazione fra le autorità pubbliche, responsabili dell'esecuzione della normativa in materia di tutela degli interessi dei consumatori, nel trattamento delle infrazioni intracomunitarie, contribuire al buon funzionamento del mercato interno, al miglioramento della qualità e della coerenza dell'applicazione delle leggi che tutelano gli interessi dei consumatori, al monitoraggio della protezione degli interessi economici dei consumatori e contribuire ad accrescere l'efficacia e la coerenza degli interventi».

— valutare se sia necessario conservare tutte le informazioni previste attualmente o se un sottoinsieme di informazioni sarebbe sufficiente (ad esempio si dovrebbe valutare se sarebbe sufficiente conservare solo le notifiche di cui all'articolo 8, paragrafo 6; si potrebbe inoltre valutare specificamente se sia necessario conservare i nomi dei direttori o i documenti che potrebbero contenere dati personali aggiuntivi nonché operare una distinzione tra i dati riguardanti i sospetti di infrazioni e le infrazioni «accertate»).

3.2. Accesso della Commissione ai dati del CPCS

38. Il GEPD si compiace che (introducendo il nuovo punto 4.3 all'allegato della decisione di attuazione CPC) la seconda modifica CPC chiarisca le modalità di accesso della Commissione ai dati del CPCS e che tale accesso sia chiaramente e specificamente limitato a quanto previsto dal regolamento CPC. In particolare, il GEPD rileva con piacere che alla Commissione non è stato fornito accesso alle comunicazioni riservate tra le autorità competenti degli Stati membri, quali le richieste di assistenza reciproca.

39. Si tratta di un chiarimento e di una limitazione particolarmente importanti, poiché la mancanza di chiarezza avrebbe potuto determinare una situazione in cui la Commissione sarebbe stata in grado di accedere a informazioni, compresi dati personali, i cui destinatari sono esclusivamente le autorità competenti degli Stati membri.

40. Come descritto alla sezione 5 delle linee guida CPC per la protezione dei dati, «l'accesso della Commissione ha come scopo il controllo dell'applicazione del regolamento CPC e della normativa, indicata nel suo allegato, concernente la tutela dei consumatori nonché la compilazione dei dati statistici relativi all'esecuzione di questi compiti».

41. Questo non significa che la Commissione deve avere accesso a tutti i dati scambiati tra gli Stati membri nell'ambito del CPCS.

42. Di fatto, il GEPD sottolinea che l'accesso a banche dati quali il CPCS rientra nella definizione di trattamento dei dati personali. A norma dell'articolo 5, lettera a), del regolamento (CE) n. 45/2001, che è pertinente per i diritti di accesso della Commissione ai dati del CPCS, il trattamento dei dati personali da parte delle istituzioni può essere effettuato soltanto quando è necessario per l'esecuzione di una funzione di interesse pubblico e purché sia realizzato sulla base dei trattati o del diritto derivato.

43. Da queste prescrizioni — che derivano direttamente dal diritto alla protezione dei dati sancito dall'articolo 8 della Convenzione europea dei diritti dell'uomo e dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea — il GEPD conclude che la Commissione può essere autorizzata ad accedere ai sistemi di informazione degli Stati membri solo qualora ciò sia previsto da disposizioni normative specifiche, fondate su una base giuridica pienamente appropriata (di norma la procedura legislativa ordinaria). La certezza del diritto e la trasparenza sono i due valori soggiacenti che spiegano perché una base giuridica specifica e sicura per l'accesso della Commissione è una garanzia particolarmente importante per la tutela dei diritti fondamentali delle persone riguardo alla protezione dei dati.

44. Né il generale potere di controllo della Commissione quale «custode del trattato» né l'obbligo degli Stati membri di assicurare una leale cooperazione sono sufficientemente precisi da consentire alla Commissione di accedere a banche dati contenenti informazioni personali. Il principio di leale cooperazione prevede che, a determinate condizioni, gli Stati membri forniscano informazioni alla Commissione su richiesta o qualora siano tenuti a procedere in tal senso nel rispetto di una disposizione specifica. Tale principio, tuttavia, non prevede l'accesso della Commissione alle loro banche dati.

45. In tale contesto il GEPD sottolinea altresì che il regolamento CPC esclude la possibilità, per la Commissione, di accedere alle informazioni contenute nelle richieste di assistenza reciproca e di esecuzione. Gli articoli 6 e 8 del regolamento CPC designano esclusivamente l'autorità interpellata, e non la Commissione, quale destinatario di questi dati.

3.3. Categorie particolari di dati nel CPCS

46. Il GEPD si compiace che la seconda modifica CPC abbia introdotto, al punto 4.4 dell'allegato alla decisione di attuazione CPC, una disposizione volta a disciplinare il trattamento di categorie particolari di dati nel CPCS. Il GEPD accoglie con particolare favore il fatto che la disposizione limiti tale trattamento ai casi in cui esso «non impedisca» il rispetto degli obblighi di cui al regolamento CPC e che il trattamento di tali dati sia subordinato all'ulteriore condizione che sia «permesso dalla direttiva 95/46/CE».

IV. PRIVACY BY DESIGN (TUTELA DELLA VITA PRIVATA FIN DALLA PROGETTAZIONE) E RESPONSABILITÀ

47. Dopo aver affrontato, nella parte III, i problemi specifici sollevati dalla seconda modifica CPC, nelle parti IV-VI il GEPD intende richiamare l'attenzione della Commissione su alcuni altri punti che dovrebbero essere presi in considerazione per l'ulteriore sviluppo del quadro giuridico del CPCS.

4.1. Privacy by design (tutela della vita privata fin dalla progettazione)

48. Il GEPD incoraggia da tempo la Commissione e altre istituzioni dell'UE ad adottare misure tecnologiche e organizzative che integrino le disposizioni in materia di sicurezza e protezione dei dati quale parte fondamentale della progettazione e dell'attuazione dei loro sistemi di informazione («privacy by design») ⁽¹²⁾.

49. Pur riconoscendo e apprezzando il fatto che sono state adottate alcune misure in questa direzione, il GEPD raccomanda alla Commissione di valutare globalmente quali altre garanzie in materia di «privacy by design» (tutela della vita privata fin dalla progettazione) potrebbero essere incorporate nell'architettura del sistema CPCS. Tra le altre, dovrebbero essere prese in considerazione e attuate, se del caso:

- soluzioni basate sul principio della «privacy by design» (tutela della vita privata fin dalla progettazione) volte a orientare gli utenti del sistema nell'adozione di decisioni «adeguate» in materia di protezione dei dati,

- misure finalizzate ad agevolare la chiusura e la soppressione tempestiva dei casi (*idem*, sezione 3.3),

- procedure volte ad agevolare i diritti di accesso e di informazione degli interessati (*idem*, sezione 3.5),

- procedure chiare per tutte le modifiche apportate direttamente a livello di banca dati, la registrazione degli accessi, la logica sottesa all'intervento e l'approvazione a livello adeguato (*idem*, sezione 3.6); e

- la memorizzazione «cifrata» delle informazioni nella banca dati al fine di impedire l'accesso ai dati da parte degli operatori informatici (almeno per alcuni dati quali i documenti riservati) (*idem*, sezione 3.6).

4.2. Responsabilità

50. Inoltre, conformemente al principio della «responsabilità» ⁽¹³⁾, il GEPD raccomanda altresì di istituire un quadro chiaro per la responsabilità che assicuri e attesti il rispetto della protezione dei dati, ad esempio:

⁽¹²⁾ Cfr. la sezione 7 del parere del GEPD sulla comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni — «Un approccio globale alla protezione dei dati personali nell'Unione europea», emesso il 14 gennaio 2011 (http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf).

⁽¹³⁾ *Idem*.

- adottando e aggiornando, se del caso, una politica in materia di protezione dei dati che dovrà essere approvata al massimo livello dirigenziale nell'ambito della DG SANCO. Tale politica in materia di protezione dei dati dovrà altresì comprendere un piano di sicurezza (cfr. la sezione 3.6 del parere sul controllo preventivo) ⁽¹⁴⁾,
- realizzando verifiche periodiche intese a valutare l'adeguatezza e il rispetto costanti della politica in materia di protezione dei dati (compresa la verifica del piano di sicurezza, *idem*, sezione 3.6),
- pubblicando (almeno parzialmente) i risultati di queste verifiche al fine di rassicurare le parti interessate in merito al rispetto della protezione dei dati; e
- notificando le violazioni dei dati e altri incidenti riguardanti la sicurezza al responsabile della protezione dei dati della Commissione e agli interessati (nonché, se del caso, ad altre parti o autorità) ⁽¹⁵⁾.

V. TRASFERIMENTO DI DATI PERSONALI OLTRE L'UNIONE EUROPEA

5.1. Accordi bilaterali

51. L'articolo 14, paragrafo 2, del regolamento CPC stabilisce che le informazioni trasmesse ai sensi del regolamento CPC possono anche essere comunicate a un'autorità di un paese terzo da un'autorità competente, nell'ambito di un accordo bilaterale di assistenza con detto paese, purché i) l'autorità competente che ha fornito l'informazione in origine abbia dato il proprio consenso e che ii) il trasferimento sia in linea con le norme dell'UE applicabili in materia di protezione dei dati.
52. Gli articoli 25 e 26 della direttiva 95/46/CE fissano determinate condizioni aggiuntive per il trasferimento di dati verso paesi terzi. Tali condizioni sono volte ad assicurare l'adeguata protezione dei dati all'estero. Inoltre prevedono anche una serie di deroghe. L'attuazione e l'interpretazione di queste disposizioni della direttiva 95/46/CE possono variare da uno Stato membro all'altro.
53. Alla luce delle precedenti considerazioni, il GEPD può accettare le garanzie incluse nel regolamento CPC, ossia che tutti i trasferimenti di dati verso paesi terzi siano soggetti i)

⁽¹⁴⁾ La Commissione dovrebbe inoltre prendere in considerazione l'ipotesi, se del caso, di realizzare almeno una valutazione parziale dell'impatto sulla protezione dei dati e della vita privata al fine di esaminare lo scopo, la durata e le modalità del periodo di conservazione ed eventualmente discutere altre questioni in sospeso che non sono ancora state affrontate approfonditamente.

⁽¹⁵⁾ Cfr. la sezione 6.3 del parere del GEPD del 14 gennaio 2011 citato in precedenza.

al consenso dell'autorità competente che ha fornito l'informazione in origine nonché ii) alle norme UE applicabili in materia di protezione dei dati.

54. Il GEPD si compiace inoltre che le linee guida CPC per la protezione dei dati raccomandino che, a meno che il paese terzo assicuri un livello adeguato di protezione dei dati, qualsiasi accordo di assistenza bilaterale preveda adeguate garanzie di protezione dei dati e — laddove ciò sia necessario — sia anche notificato alle autorità competenti per la protezione dei dati.
55. Detto ciò, gli accordi previsti nel regolamento CPC non sono ideali. La loro applicazione è complessa: per decidere in merito al trasferimento di informazioni verso un paese terzo, un'autorità competente dovrà tenere conto non solo dell'accordo bilaterale del suo paese con il paese terzo, delle norme nazionali in materia di protezione dei dati e della propria valutazione dell'adeguatezza del trasferimento dei dati verso il paese terzo in questione in base alla legislazione in materia di protezione dei dati del proprio paese, ma dovrà anche valutare se le altre autorità competenti interessate che hanno contribuito al fascicolo (e può esservene più di una) hanno fornito il proprio consenso sulla base delle norme vigenti in materia di protezione dei dati nel loro paese.
56. Dal punto di vista della protezione dei dati, questa complessità determina incertezze per quanto riguarda i diritti dell'interessato e, in particolare, incertezze in merito alle eventuali condizioni alle quali i suoi dati verranno trasferiti all'estero. Gli interessati, inoltre, non beneficiano nella massima misura possibile di una normativa europea solida e armonizzata in materia di protezione dei dati. Per quanto riguarda le autorità competenti, inoltre, è probabile che tale complessità ne ostacoli la cooperazione, oltre a costituire un onere amministrativo.
57. Alla luce delle precedenti considerazioni, il GEPD incoraggia la conclusione di accordi a livello dell'UE che forniscano garanzie adeguate in materia di protezione dei dati e, al contempo, contribuiscano altresì a evitare l'applicazione di criteri eterogenei nonché il conseguente aumento degli oneri amministrativi a carico delle autorità competenti.

5.2. Accordi a livello dell'UE

58. Oltre alla possibilità di cooperazione bilaterale prevista dall'articolo 14, l'articolo 18 del regolamento CPC sugli accordi internazionali stabilisce altresì che la «Comunità collabora con i paesi terzi e con le organizzazioni internazionali competenti» e che «le disposizioni relative alla cooperazione, comprese quelle relative alla definizione di accordi di assistenza reciproca, possono formare oggetto di accordi fra la Comunità e i paesi terzi interessati».

59. Per i motivi illustrati nella precedente sezione 5.1, il GEPD appoggia l'iniziativa della Commissione di negoziare e concludere accordi a livello dell'UE, contenenti adeguate garanzie in materia di protezione dei dati, armonizzate a livello dell'UE, al fine di sostituire gli accordi bilaterali esistenti.
60. Il suo sostegno a favore di tali accordi a livello dell'UE è tuttavia subordinato all'impegno della Commissione e dei legislatori dell'Unione ad assicurare il massimo livello di protezione per gli scambi di dati personali con i paesi terzi. Le implicazioni degli accordi di cooperazione internazionale con i paesi terzi devono essere prese attentamente in considerazione dal punto di vista della protezione dei dati; devono essere fissate norme chiare che disciplinino questi scambi e fornite adeguate garanzie in materia di protezione dei dati, sulla base della consultazione del GEPD e, se del caso, delle autorità nazionali di protezione dei dati.
61. Benché l'articolo 18 del regolamento CPC non affronti espressamente la questione dell'accesso diretto al CPCS da parte delle autorità dei paesi terzi, questo può essere tecnicamente possibile. Il GEPD non intende scoraggiare l'inclusione di nuove funzionalità nel CPCS volte a consentire alle autorità competenti dei paesi terzi un accesso rigorosamente limitato e selettivo tramite un meccanismo specificamente concepito (canale e interfaccia di comunicazione). Tale misura potrebbe effettivamente accrescere l'efficienza della cooperazione.
62. Detto ciò, un accesso diretto di questo tipo ha i suoi rischi e, di conseguenza, occorre considerare specificamente le sue implicazioni per la protezione dei dati nonché le necessarie garanzie e modalità tecniche/organizzative. Tali eventuali funzionalità tecniche devono essere create utilizzando i principi della «privacy by design» (tutela della vita privata fin dalla progettazione). Anche la sicurezza deve essere una priorità chiara. Infine devono essere consultati sia il GEPD sia, se del caso, le autorità nazionali di protezione dei dati.
63. Il GEPD è fiducioso che, se le sue raccomandazioni (comprese quelle formulate nel parere sul controllo preventivo) verranno seguite, il CPCS può essere uno strumento efficace e funzionale alla protezione dei dati per l'applicazione transfrontaliera della normativa volta a contrastare le infrazioni dei diritti dei consumatori nel mercato interno.
64. Con lo sviluppo del commercio elettronico e il crescente utilizzo delle reti di comunicazione elettronica da parte di fruitori di vari prodotti e servizi, verrà trattato un numero sempre maggiore di dati personali dei consumatori. Questi ultimi, pertanto, potranno anche essere sempre più esposti a infrazioni dei loro diritti in materia di protezione dei dati. Di conseguenza sussiste altresì la necessità di una cooperazione efficace tra le autorità di protezione dei dati volta a porre fine a tali infrazioni.
65. Tra i casi più comuni di violazione di «diritti relativi alla protezione dei dati dei consumatori» figurano comunicazioni commerciali indesiderate (spam), furto di identità, profilazione illecita, pubblicità comportamentale illegale e violazioni dei dati (violazioni della sicurezza).
66. Poiché nella società dell'informazione il numero di casi di natura transfrontaliera è probabilmente destinato ad aumentare, il GEPD incoraggia la Commissione a considerare possibili misure legislative volte a tutelare i «diritti relativi alla protezione dei dati dei consumatori» nonché a rafforzare la cooperazione transfrontaliera tra le autorità competenti: sia le autorità garanti della protezione dei dati sia le autorità responsabili della tutela dei consumatori.
67. In particolare, e considerando anche altre opzioni possibili, occorre valutare attentamente l'opportunità di concedere alle autorità di protezione dei dati un accesso su misura al CPCS affinché possano cooperare tra loro e con altre autorità competenti che hanno già accesso al CPCS.
68. L'accesso da parte delle autorità di protezione dei dati deve essere chiaramente limitato a quanto necessario per l'assolvimento dei loro doveri nell'ambito delle rispettive aree di competenza e conforme alle sinergie individuate. Ovviamente è altresì necessario garantire che il quadro per la partecipazione delle autorità di protezione dei dati sia concepito in modo tale che venga tenuta nella debita considerazione la loro indipendenza.

VII. CONCLUSIONI

- VI. «DIRITTI RELATIVI ALLA PROTEZIONE DEI DATI DEI CONSUMATORI» E COOPERAZIONE RAFFORZATA, TRAMITE IL CPCS, DELLE AUTORITÀ DI PROTEZIONE DEI DATI**
69. Il GEPD constata con piacere che il CPCS si fonda su una base giuridica che prevede anche garanzie specifiche in materia di protezione dei dati. Il GEPD rileva che, per affrontare le eventuali questioni irrisolte in materia di protezione dei dati, in occasione della prossima revisione del quadro giuridico del CPCS dovranno essere prese in considerazione le raccomandazioni brevemente riportate di seguito.
70. Nel frattempo, misure supplementari adottate a livello pratico, tecnico e organizzativo (raccomandate nel parere sul controllo preventivo) potrebbero fornire una soluzione temporanea parziale a questi problemi. In attesa delle modifiche legislative, potrebbero essere introdotte alcune modifiche anche tramite le linee guida CPC per la protezione dei dati.

71. Per quanto riguarda il periodo di conservazione, il GEPD raccomanda i) la chiusura delle richieste di assistenza reciproca entro termini espressamente fissati; ii) a meno che l'indagine o l'azione di esecuzione siano in corso, il ritiro e la soppressione degli allarmi entro sei mesi dalla loro trasmissione (salvo che sia possibile giustificare un altro periodo di conservazione più appropriato); e iii) alla Commissione di chiarire e riconsiderare lo scopo e la proporzionalità della conservazione di tutti i dati relativi ai casi chiusi per altri cinque anni.
72. Inoltre, il GEPD si compiace che la seconda modifica CPC chiarisca le modalità di accesso della Commissione ai dati del CPS. In particolare, il GEPD rileva con piacere che la Commissione non ha accesso alle comunicazioni riservate tra le autorità competenti degli Stati membri, quali le richieste di assistenza reciproca.
73. Il GEPD si compiace inoltre che la seconda modifica CPC abbia introdotto una disposizione volta a disciplinare il trattamento di categorie particolari di dati nel CPCS.
74. Come osservazioni aggiuntive, il GEPD raccomanda alla Commissione di rivalutare quali altre misure tecniche e organizzative adottare al fine di «incorporare» la protezione della vita privata e dei dati nell'architettura del sistema CPCS («privacy by design») nonché di prevedere controlli adeguati volti a garantire e attestare il rispetto della protezione dei dati («responsabilità»).
75. Inoltre, qualora sia necessario concludere un accordo a livello dell'UE tra l'Unione europea e un paese terzo al fine di disciplinare la cooperazione per la tutela dei consumatori, occorrerà prendere attentamente in considerazione le implicazioni di tali accordi, fissare norme chiare che disciplinino gli scambi in questione e fornire adeguate garanzie in materia di protezione dei dati.
76. Infine, il GEPD raccomanda alla Commissione di esplorare le eventuali sinergie che potrebbero scaturire qualora alle autorità di protezione dei dati venisse consentito di unirsi alla comunità degli utenti del CPCS al fine di contribuire all'applicazione dei «diritti relativi alla protezione dei dati dei consumatori».

Fatto a Bruxelles, il 5 maggio 2011.

Giovanni BUTTARELLI

Garante europeo aggiunto della protezione dei dati
