

GARANTE EUROPEO DELLA PROTEZIONE DEI DATI

Sintesi del parere del Garante europeo della protezione dei dati sulla comunicazione della Commissione «Sfruttare il potenziale del cloud computing in Europa»

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

(2013/C 253/03)

I. Introduzione

I.1. Obiettivo del parere

1. Alla luce dell'importanza del «cloud computing» (nuvola informatica) nella società dell'informazione in evoluzione e del dibattito politico in corso nell'Unione europea sul cloud computing, il GEPD ha deciso di formulare il presente parere di propria iniziativa.

2. Il presente parere risponde alla comunicazione della Commissione «Sfruttare il potenziale del cloud computing in Europa», del 27 settembre 2012 (in prosieguo «la comunicazione») ⁽¹⁾, che definisce le azioni fondamentali e gli interventi strategici da adottare per accelerare l'utilizzo dei servizi di cloud computing in Europa. Prima dell'adozione della comunicazione il GEPD era stato consultato e aveva formulato osservazioni in modo informale. Il GEPD è lieto di constatare che alcune delle sue osservazioni sono state prese in considerazione nella comunicazione.

3. Tuttavia, considerate la portata e l'importanza del dibattito in corso sulla relazione tra il cloud computing e il quadro giuridico sulla protezione dei dati, il presente parere non si limita agli argomenti affrontati nella comunicazione.

4. Il parere si concentra in particolare sulle sfide che il cloud computing comporta per la protezione dei dati e sul modo in cui la proposta di regolamento sulla protezione dei dati (in prosieguo «la proposta di regolamento») ⁽²⁾ le affronterà. Formula inoltre osservazioni sui settori di azione prioritari individuati nella comunicazione.

I.2. Contesto

5. Nel contesto del dibattito politico generale in corso nell'UE sul cloud computing, risultano particolarmente importanti le attività e i documenti elencati di seguito:

— successivamente alla sua comunicazione del 2010 sull'agenda digitale europea ⁽³⁾, la Commissione ha avviato una consultazione pubblica sul cloud computing in Europa dal 16 maggio al 31 agosto 2011 e ha pubblicato i risultati il 5 dicembre 2011 ⁽⁴⁾;

— il 1° luglio 2012 il gruppo di lavoro «articolo 29» ⁽⁵⁾ ha adottato un parere sul cloud computing (in prosieguo il «parere del gruppo di lavoro «articolo 29»») ⁽⁶⁾, che analizza l'applicazione delle norme vigenti in materia di protezione dei dati enunciate nella direttiva 95/46/CE ai fornitori di servizi di cloud computing operanti nello Spazio economico europeo (SEE) e ai loro clienti ⁽⁷⁾;

— il 26 ottobre 2012 i commissari in materia di protezione dei dati e della vita privata hanno adottato una risoluzione sul cloud computing in occasione della loro 34^a conferenza internazionale ⁽⁸⁾.

⁽¹⁾ COM(2012) 529 final.

⁽²⁾ COM(2012) 11 final.

⁽³⁾ COM(2010) 245 definitivo.

⁽⁴⁾ http://ec.europa.eu/information_society/activities/cloudcomputing/docs/ccconsultationfinalreport.pdf

⁽⁵⁾ Il gruppo di lavoro «articolo 29» è un organo consultivo istituito in virtù dell'articolo 29 della direttiva 95/46/CE. È composto da rappresentanti delle autorità di controllo nazionali e del GEPD nonché da un rappresentante della Commissione.

⁽⁶⁾ Parere del gruppo di lavoro «articolo 29» sul *cloud computing*, disponibile all'indirizzo: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_it.pdf

⁽⁷⁾ Inoltre, a livello nazionale le autorità di protezione dei dati di alcuni Stati membri hanno formulato le proprie indicazioni per l'utilizzo dei servizi di cloud computing, come è avvenuto ad esempio in Italia, Svezia, Danimarca, Germania, Francia e Regno Unito.

⁽⁸⁾ Risoluzione sul cloud computing adottata durante la 34^a conferenza internazionale dei commissari in materia di protezione dei dati e della vita privata, Uruguay, 26 ottobre 2012.

I.3. Comunicazione sul cloud computing

6. Il GEPD accoglie con favore la comunicazione. Individua tre azioni fondamentali specifiche necessarie a livello UE per accompagnare e promuovere l'utilizzo del cloud computing in Europa:

- azione fondamentale 1: districare il groviglio di norme
- azione fondamentale 2: rendere sicure ed eque le clausole contrattuali
- azione fondamentale 3: istituire un partenariato europeo per il cloud che faccia del settore pubblico il motore dell'innovazione e della crescita.

7. Sono previsti anche ulteriori interventi strategici, quali misure volte a incentivare l'utilizzo del cloud computing favorendo la ricerca e lo sviluppo o azioni di sensibilizzazione, nonché la necessità di affrontare temi fondamentali legati ai servizi di cloud — tra cui, ad esempio, la protezione dei dati, l'accesso ai dati da parte degli organi incaricati dell'applicazione della legge, la sicurezza, la responsabilità dei fornitori intermediari di servizi — tramite un dialogo internazionale rafforzato.

8. La comunicazione considera la protezione dei dati un elemento essenziale per garantire il successo dell'utilizzo del cloud computing in Europa. La comunicazione rileva ⁽¹⁾ che la proposta di regolamento affronta molte delle preoccupazioni sollevate dai fornitori di servizi di cloud e dai clienti cloud ⁽²⁾.

I.4. Fulcro e struttura del parere

9. Il presente parere ha tre obiettivi.

10. Il primo obiettivo è evidenziare l'importanza della protezione della vita privata e dei dati personali nelle attuali discussioni sul cloud computing. Più specificamente, il presente parere sottolinea che il livello di protezione dei dati in un ambiente di cloud computing non deve essere inferiore a quello necessario in qualsiasi altro contesto di trattamento dei dati. Le pratiche di cloud computing possono essere sviluppate e applicate legalmente solo se garantiscono il rispetto di tale livello di protezione dei dati (cfr. il capitolo III.3). Il parere tiene conto delle indicazioni fornite nel parere del gruppo di lavoro «articolo 29».

11. Il secondo obiettivo è analizzare ulteriormente le sfide principali che il cloud computing comporta per la protezione dei dati nel contesto della proposta di regolamento sulla protezione dei dati, in particolare la difficoltà di definire chiaramente le responsabilità dei differenti attori nonché i concetti di responsabile del trattamento e incaricato del trattamento. Il parere (principalmente il capitolo IV) analizza il modo in cui la proposta di regolamento, nella sua formulazione attuale ⁽³⁾, contribuirà a garantire un livello elevato di protezione dei dati nei servizi di cloud computing. Si basa pertanto sulle osservazioni formulate dal GEPD nel suo parere sul pacchetto di riforma della protezione dei dati (in prosieguo «il parere del GEPD sul pacchetto di riforma della protezione dei dati») ⁽⁴⁾ e lo integra prendendo specificamente in considerazione l'ambiente del cloud computing. Il GEPD sottolinea che il suo parere sul pacchetto di riforma della protezione dei dati si applica appieno ai servizi di cloud computing e deve essere considerato come base del presente parere. Inoltre, alcune delle questioni affrontate in tale documento — quale la sua analisi delle nuove disposizioni sui diritti degli interessati ⁽⁵⁾ — sono sufficientemente chiare e pertanto non saranno ulteriormente sviluppate nel presente parere.

12. Il terzo obiettivo è individuare i settori che richiedono ulteriori interventi a livello UE dal punto di vista della protezione dei dati e della vita privata, alla luce della strategia di cloud computing enunciata dalla Commissione nella comunicazione. Tra questi figurano, ad esempio, la fornitura di ulteriori orientamenti, iniziative a favore della normazione, lo svolgimento di ulteriori valutazioni dei rischi per settori specifici (quali il settore pubblico), l'elaborazione di clausole contrattuali tipo, l'avvio di un dialogo internazionale su questioni inerenti il cloud computing e la capacità di garantire strumenti efficaci di cooperazione internazionale (argomento che sarà sviluppato nel capitolo V).

⁽¹⁾ Cfr. la sezione «Le azioni dell'Agenda digitale per «ispirare fiducia nel digitale», a pagina 8 della comunicazione.

⁽²⁾ Nel presente parere l'espressione «clienti cloud» viene generalmente utilizzata in riferimento a clienti che agiscono in qualità di imprese e a consumatori che agiscono in qualità di singoli utenti finali.

⁽³⁾ Occorre tenere conto del fatto che la proposta di regolamento è attualmente oggetto di discussione da parte del Consiglio e del Parlamento europeo secondo la procedura legislativa ordinaria.

⁽⁴⁾ Il parere è disponibile all'indirizzo <http://www.edps.europa.eu>

⁽⁵⁾ Cfr. il parere del GEPD, in particolare i paragrafi 140-158.

13. Il parere è strutturato come segue: la sezione II fornisce una panoramica delle caratteristiche principali del cloud computing e delle sfide che questa tecnologia comporta per la protezione dei dati. La sezione III passa in rassegna gli elementi più rilevanti dell'attuale quadro giuridico dell'UE e della proposta di regolamento. La sezione IV analizza il modo in cui la proposta di regolamento contribuirà ad affrontare le sfide che l'utilizzo dei servizi di cloud computing comporta per la protezione dei dati. La sezione V analizza i suggerimenti della Commissione per gli sviluppi politici futuri e individua i settori in cui potrebbero essere necessari ulteriori approfondimenti. La sezione VI contiene le conclusioni.

14. Benché molte delle considerazioni contenute nel presente documento si applichino a tutti gli ambienti in cui viene utilizzato il cloud computing, questo parere non affronta la questione dell'utilizzo dei servizi di cloud computing specificamente da parte delle istituzioni e degli organismi dell'UE soggetti al controllo del GEPD ai sensi del regolamento (CE) n. 45/2001. Il GEPD formulerà separatamente orientamenti sull'argomento destinati a tali istituzioni e organismi.

VI. Conclusioni

121. Come indicato nella comunicazione, il cloud computing offre molte nuove possibilità sia a imprese e consumatori che al settore pubblico per la gestione di dati tramite l'utilizzo di risorse informatiche esterne in remoto. Al tempo stesso, presenta molte sfide, in particolare per quanto riguarda il livello appropriato di protezione dei dati offerto ai dati trattati in tale contesto.

122. L'utilizzo dei servizi di cloud computing presenta un rischio considerevole di assistere a una evaporazione della responsabilità per quanto riguarda le operazioni di trattamento svolte dai fornitori di servizi di cloud, qualora i criteri di applicabilità della normativa UE in materia di protezione dei dati non siano sufficientemente chiari nonché nel caso in cui il ruolo e la responsabilità dei fornitori di servizi di cloud siano definiti o interpretati in modo troppo restrittivo o non siano attuati in maniera efficace. Il GEPD sottolinea che l'utilizzo dei servizi di cloud computing non può giustificare un abbassamento degli standard di protezione dei dati rispetto a quelli applicabili alle procedure tradizionali di trattamento dei dati.

123. A tale proposito la proposta di regolamento sulla protezione dei dati, nella sua formulazione attuale, fornirà molti chiarimenti e strumenti che contribuiranno a garantire il rispetto di un livello soddisfacente di protezione dei dati da parte dei fornitori di servizi di cloud che offrono i loro servizi a clienti stabiliti in Europa, in particolare:

- l'articolo 3 preciserà il campo di applicazione territoriale delle norme UE in materia di protezione dei dati e ampliarà il proprio ambito di applicazione in modo da includere i servizi di cloud computing;
- l'articolo 4, paragrafo 5, introdurrà un nuovo elemento di responsabilità, ossia le «condizioni», in linea con la tendenza in via di sviluppo secondo cui, alla luce della complessità informatica tecnica sottesa alla fornitura di servizi di cloud computing, è necessario ampliare i casi in cui un fornitore di servizi di cloud può essere definito responsabile del trattamento. Ciò rispecchierà meglio l'effettivo livello di influenza sulle operazioni di trattamento;
- la proposta di regolamento aumenterà la responsabilità dei responsabili del trattamento e degli incaricati del trattamento dei dati, introducendo obblighi specifici quali la protezione dei dati fin dalla progettazione («by design») e la protezione di default (articolo 23), la notifica delle violazioni della sicurezza dei dati (articoli 31 e 32) nonché valutazioni d'impatto in materia di protezione dei dati (articolo 33). Inoltre, imporrà a responsabili del trattamento e incaricati del trattamento l'obbligo di realizzare meccanismi atti a dimostrare l'efficacia delle misure di protezione dei dati attuate (articolo 22);
- gli articoli 42 e 43 della proposta di regolamento consentiranno un utilizzo più flessibile dei meccanismi per il trasferimento internazionale di dati, al fine di aiutare i clienti cloud e i fornitori di servizi di cloud a offrire garanzie adeguate in materia di protezione dei dati per i trasferimenti di dati personali a centri di trattamento dati o a server situati in paesi terzi;
- gli articoli 30, 31 e 32 della proposta di regolamento preciseranno gli obblighi dei responsabili del trattamento e degli incaricati del trattamento riguardo alla sicurezza dei trattamenti nonché gli obblighi di informazione in caso di violazioni di dati, ponendo le basi per un approccio globale e cooperativo alla gestione della sicurezza tra i differenti attori in un ambiente di cloud;

— gli articoli 55-63 della proposta di regolamento rafforzeranno la cooperazione delle autorità di controllo e il loro controllo coordinato sui trattamenti transfrontalieri, che è determinante in un ambiente come il cloud computing.

124. Il GEPD suggerisce tuttavia che, dopo aver preso in considerazione le specificità dei servizi di cloud computing, siano apportati ulteriori chiarimenti alla proposta di regolamento sui seguenti aspetti:

- per quanto riguarda l'ambito di applicazione territoriale della proposta di regolamento, modificare nel seguente modo l'articolo 3, paragrafo 2, lettera a): «l'offerta di beni o la prestazione di servizi *che comportano il trattamento di dati personali dei* suddetti residenti nell'Unione» o, in alternativa, aggiungere un nuovo considerando in cui si specifichi che il trattamento dei dati personali di residenti nell'Unione da parte di responsabili del trattamento non stabiliti nell'UE che offrono servizi a persone giuridiche stabilite nell'Unione rientra a sua volta nell'ambito di applicazione territoriale della proposta di regolamento;
- aggiungere una definizione chiara del concetto di «trasferimento», quale fornita dal GEPD nel suo parere sul pacchetto di riforma della protezione dei dati;
- aggiungere una disposizione specifica volta a precisare le condizioni alle quali potrebbe essere consentito l'accesso ai dati conservati nei servizi di cloud computing da parte degli organi incaricati dell'applicazione della legge dei paesi non facenti parte del SEE. Tale disposizione potrebbe prevedere anche l'obbligo per il destinatario della richiesta di informare e consultare l'autorità di controllo competente nell'UE in casi specifici.

125. Il GEPD sottolinea inoltre che la Commissione e/o altre autorità di controllo dovranno fornire ulteriori orientamenti (in particolare tramite il futuro comitato europeo per la protezione dei dati) sui seguenti aspetti:

- precisare quali meccanismi dovranno essere attuati per garantire la verifica dell'efficacia delle misure di protezione dei dati nella pratica;
- aiutare gli incaricati del trattamento nell'utilizzo delle norme vincolanti d'impresa indicando altresì loro il modo in cui possono rispettare gli obblighi stabiliti;
- fornire esempi di buone pratiche su questioni quali la responsabilità del responsabile/dell'incaricato del trattamento, l'adeguata conservazione dei dati nell'ambiente di cloud, la portabilità dei dati e l'esercizio dei diritti degli interessati.

126. Il GEPD riconosce inoltre che i codici di condotta elaborati dal settore e approvati dalle autorità di controllo competenti potrebbero rivelarsi uno strumento utile per migliorare il rispetto delle norme e aumentare la fiducia tra i vari attori.

127. Il GEPD sostiene lo sviluppo da parte della Commissione, in consultazione con le autorità di controllo, di clausole contrattuali tipo per la fornitura di servizi di cloud computing che rispettino gli obblighi in materia di protezione dei dati, in particolare:

- elaborare clausole contrattuali tipo da inserire nelle clausole commerciali delle offerte di servizi di cloud computing;
- elaborare condizioni contrattuali comuni relative agli appalti per il settore pubblico, tenendo conto della sensibilità dei dati trattati;
- adeguare ulteriormente i meccanismi per il trasferimento internazionale di dati all'ambiente del cloud computing, in particolare aggiornando le attuali clausole contrattuali tipo e proponendo clausole contrattuali tipo per il trasferimento di dati dagli incaricati del trattamento stabiliti nell'UE agli incaricati del trattamento situati al di fuori dell'UE.

128. Il GEPD sottolinea che occorre tenere in debita considerazione gli obblighi in materia di protezione dei dati nello sviluppo di norme e regimi di certificazione, in particolare:

- applicare i principi della protezione dei dati fin dalla progettazione («by design») e della protezione di default nello sviluppo delle norme;
- integrare obblighi in materia di protezione dei dati quali la limitazione delle finalità e la limitazione della conservazione nella progettazione delle norme;
- prevedere l'obbligo per i fornitori sia di dare ai loro clienti le informazioni necessarie all'esecuzione di una valutazione dei rischi valida nonché le informazioni relative alle misure di sicurezza attuate, sia di segnalare gli incidenti inerenti la sicurezza.

129. Infine, il GEPD sottolinea la necessità di affrontare le sfide poste dal cloud computing a livello internazionale. Incoraggia la Commissione ad avviare un dialogo internazionale sulle questioni sollevate dal cloud computing, tra cui la giurisdizione e l'accesso ai dati da parte degli organi incaricati dell'applicazione della legge, e suggerisce che molte di tali questioni potrebbero essere affrontate nell'ambito di differenti accordi internazionali o bilaterali, quali gli accordi di mutua assistenza nonché gli accordi commerciali. E' necessario sviluppare norme globali a livello internazionale al fine di definire condizioni minime e principi riguardanti l'accesso ai dati da parte degli organi incaricati dell'applicazione della legge. Il GEPD sostiene inoltre lo sviluppo di meccanismi di cooperazione internazionale efficaci da parte delle autorità di controllo, in particolare per quanto riguarda le questioni relative al cloud computing.

Fatto a Bruxelles, il 16 novembre 2012

Peter HUSTINX
Garante europeo della protezione dei dati
