DOI: 10.26314/GARR-Conf17-proceedings-09

Il nuovo Regolamento Privacy, cloud computing e big data

Nadina Foggetti

Università degli Studi di Bari, Dipartimento di Giurisprudenza

Abstract. Il primo aspetto che esamineremo riguarda le problematiche connesse alla privacy. Il trattamento dei dati personali assume particolari peculiarità a seconda della tipologia di cloud computing che prendiamo in considerazione. In particolare si prenderanno in considerazione le problematiche connesse al maggiore livello di responsabilizzazione dei responsabili del trattamento, mediante l'introduzione di un sistema innovativo di valutazione dei rischi connessi alla tutela dei dati personali. Nel cloud computing si può qualificare l'attività svolta rispetto al trattamento di dati come "data processor", tuttavia nella prassi, le attività svolte sono maggiormente inquadrabili nell'ambito di quelle garantite da un "responsabile del trattamento". Il secondo obiettivo riguarda la disciplina giuridica del trattamento dei Big Data nel diritto internazionale e dell'UE. Gli aspetti di rilievo che occorre analizzare riguardano la Data discovery, la raccolta e la profilazione alla luce della disciplina vigente a livello europeo ed internazionale. I Big Data introducono una rivoluzione significativa in materia di privacy inserendosi in un settore caratterizzato già da un'elevata complessità e pongono la questione relativa alla definizione degli scopi perseguiti attraverso la raccolta e il trattamento dei dati stessi, ovvero quale sia la tipologia dei dati trattati e quindi la relativa disciplina. L'analisi verrà condotta alla luce del Reg. 2016/679 del 27 aprile 2016.

Keywords. Big Data, Privacy, RGPD, Cloud Computing.

Introduzione

La libera circolazione dei dati è al centro del nuovo Regolamento privacy dell'UE (RGPD). La nuova disciplina uniforma di fatto la normativa in materia di privacy a livello europeo ed è orientata ad accogliere le nuove sfide della società dell'informazione, tra cui in particolare la profilazione, i Big Data ed il diritto all'oblio.

1.Big data e profilazione

La tecnologia cloud ha contribuito a determinare la diffusione dei Big Data. Il WP29 definisce i Big Data come "gigantesche banche dati digitali ... analizzate in modo estensivo attraverso algoritmi elettronici". I Big Data introducono una rivoluzione in materia di privacy inserendosi in un settore caratterizzato già da un'elevata complessità. Spesso, come avviene ad esempio nell'ambito della bioinformatica, i dati prodotti a seguito del trattamento, possono avere una natura giuridica differente rispetto a quella attribuibile ai dati inizialmente raccolti o forniti dall'interessato. Il RGPD introduce il diritto dell'interessato a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici nei suoi confronti,

a meno che non sia necessaria per la conclusione o l'esecuzione di un contratto tra lo stesso e un titolare del trattamento; non sia autorizzata dal diritto; o si basi sul consenso dell'interessato. Il Regolamento introduce un obbligo specifico per il titolare del trattamento di effettuare una valutazione di impatto (DPIA), qualora vi sia un trattamento sistematico e globale di aspetti personali relativi a persone fisiche, basato su un sistema automatizzato, compresa la profilazione.

Il RGPD impone ai titolari di adottare misure atte a dimostrare la compliance normativa, tenendo conto dei "rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche". L'obbligo di condurre una DPIA è collocato nel contesto della responsabilità di gestire correttamente i rischi connessi al trattamento di dati personali. Per "rischio" si intende uno scenario descrittivo di un evento e delle conseguenze che sono stimate in termini di gravità e probabilità. La "gestione del rischio" è definibile come l'insieme coordinato delle attività finalizzate a guidare e monitorare un ente o organismo nei riguardi di tale rischio.

Il riferimento ai "diritti e le libertà" degli interessati afferisce innanzitutto al diritto alla privacy, ma può riguardare anche altri diritti fondamentali quali la libertà di espressione e di pensiero. Coerentemente con l'approccio basato sul rischio che informa il Regolamento, la DPIA è obbligatoria solo se una determinata tipologia di trattamenti "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (art. 35, paragrafo 1). Anche in assenza delle circostanze che impongono l'adozione di una DPIA, i titolari devono valutare in modo continuativo i rischi creati dai propri trattamenti così da individuare quelle situazioni in cui una determinata tipologia di trattamenti "può presentare un rischio elevato".

L'elenco disposto dall'art. 35 non è esaustivo, possono esservi trattamenti "a rischio elevato" non ricompresi nell'elenco, per questo il WP29 ha specificato dei sub criteri da considerare nella valutazione del rischio quali l'esistenza di trattamenti di scoring, compresa la profilazione e attività predittive, in particolare a partire da "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali", come ad esempio una società biotecnologica che somministri test genetici gratuiti ai consumatori per finalità predittive del rischio di determinate patologie. Un ulteriore criterio è rappresentato dal monitoraggio sistematico quali "la sorveglianza metodica di un'area accessibile al pubblico". Un altro criterio riguarda i trattamenti di dati su larga scala. Il WP29 ha stabilito che è opportuno tenere conto di alcuni indicatori quali il numero di soggetti interessati; il volume dei dati e/o ambito delle diverse tipologie; la durata; l'ambito geografico.

Nella valutazione del rischio occorre considerare se vi sia una combinazione o raffronto di insiemi di dati, per esempio derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato. Infine occorre considerare l'esistenza di dati relativi a interessati vulnerabili poiché in questa situazione risulta accentuato lo squilibrio di poteri fra interessato e titolare. Il Regolamento prevede il "rischio del trattamento", inteso come l'impatto negativo sulle libertà e i diritti degli interessati. Si tratta di un approccio

risk based, che ha il vantaggio di pretendere degli obblighi che possono andare oltre la compliance, più adattabile al mutare degli strumenti tecnologici, ma che delega al titolare del trattamento la valutazione del rischio, rendendo più difficili le contestazioni in caso di violazioni.

2. I nuovi diritti introdotti

L'articolo 20 del RGPD introduce il diritto alla portabilità dei dati, che permette agli interessati di ricevere i dati personali, in un formato strutturato, di uso comune e leggibile meccanicamente e di trasmetterli a un diverso titolare. L'obiettivo è accrescere il controllo degli interessati sui propri dati personali. Consentendo la trasmissione diretta dei dati personali da un titolare all'altro, attua il principio della libera circolazione dei dati ed è teso a garantire trasparenza nella disciplina dei contratti facilitando il passaggio da un fornitore di servizi all'altro.

Ai fini dell'applicazione del diritto è necessario il consenso dell'interessato, la presenza di un trattamento effettuato con mezzi automatizzati, non applicandosi, invece, ai registri cartacei. Il WP29 precisa che il Regolamento non prevede un diritto generale alla portabilità dei dati il cui trattamento non si fondi sul consenso o su un contratto. Il WP29 ha chiarito che il diritto alla portabilità dei dati si configura rispetto ai dati forniti consapevolmente e in modo attivo dall'interessato, nonché rispetto ai dati generati dalle attività svolte dall'interessato, diversamente la natura dello stesso risulterebbe svuotata del suo contenuto.

Il principio richiede l'adozione da parte dei titolari di dispositivi atti a facilitare l'esercizio del diritto, quali strumenti per il download dei dati e API. Vi è, infatti, l'obbligo di garantire che i dati personali siano trasmessi in un formato strutturato, accessibile, in capo ai titolari. Sarebbe pertanto necessario garantire l'adozione di un formato standard che assicuri l'interoperabilità dei formati con cui i dati sono messi a disposizione. L'innovazione apportata è funzionale a garantire un maggiore controllo dei propri dati personali, effettuando, di fatto un "bilanciamento" nel rapporto tra interessati e titolari. È possibile individuare alcuni elementi di cui il diritto in parola si compone. Include il diritto dell'interessato a ricevere un insieme di dati da un titolare al fine di conservarli in vista di un utilizzo futuro per scopi personali. La conservazione può avvenire tramite un cloud privato, senza richiedere la trasmissione dei dati ad un altro titolare, rappresentando un'estensione del diritto di accesso. Un secondo elemento è il diritto di trasmettere dati personali ad un altro titolare senza impedimenti al fine di garantire all'interessato un margine di controllo sui dati, impedendo forme di "lock-in" tecnologico. Il diritto in parola non è un diritto assoluto, poiché il suo esercizio non deve pregiudicare nessuno degli altri diritti. Qualora l'interessato intenda esercitare il diritto all'oblio, il titolare non può procrastinare o negare l'applicazione dello stesso in virtù dell'applicazione del diritto di cui all'articolo 20 del RGPD.

Un aspetto importante riguarda l'applicazione del principio ai dati generati dal titolare, per esempio mediante l'analisi di dati grezzi originati da un contatore intelligente. Occorre effettuare una distinzione tra i dati forniti dall'interessato, anche nella fruizio-

ne di un servizio e quelli forniti consapevolmente dall'interessato. Il WP29 ritiene che la nozione di dati "forniti da" un interessato debba riferirsi anche ai dati personali osservati sulla base delle attività svolte dagli utenti, come per esempio i dati grezzi generati da un contatore intelligente o altri oggetti connessi, le registrazioni delle attività svolte, la cronologia della navigazione su un sito web. L'espressione "forniti da" si riferisce ai dati personali relativi ad attività compiute dall'interessato o derivanti dall'osservazione del comportamento, con esclusione dei dati derivanti dalla successiva analisi di tale comportamento. Viceversa, tutti i dati personali che siano creati dal titolare nell'ambito di un trattamento, per esempio attraverso procedure di personalizzazione o finalizzate alla formulazione di raccomandazioni, o attraverso la categorizzazione o profilazione degli utenti, sono dati derivati o dedotti dai dati personali forniti dall'interessato e non ricadono nell'ambito del diritto alla portabilità. Il GRPD introduce una tempistica entro la quale è necessario garantire l'esercizio del diritto alla portabilità dei dati, stabilendo all'art. 12, paragrafo 3, che il titolare fornisce "informazioni relative all'azione intrapresa" all'interessato "senza ingiustificato ritardo" e comunque "entro un mese dal ricevimento dalla richiesta" che si estende previa motivazione a tre mesi in casi di particolare complessità.

3. Conclusioni

Il GRPD, in definitiva introduce una serie di diritti innovativi, quali quello alla portabilità dei dati, il diritto all'oblio ed alcuni obblighi quali quello di adozione di DPIA. Tuttavia occorre rilevare che si basa su un'ottica fondata sul consenso, apparendo di fatto maggiormente orientato alla libera circolazione dei dati e quindi alle esigenze connesse alla società dell'informazione.

Riferimenti bibliografici

E. Pelino, L. Bolognini, C. Bistolfi (2016), Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali Copertina flessibile, Milano.

R.H. JR. Carpenter (2010), Walking From Cloud To Cloud: The Portability Issue In Cloud Computing, in Washington Journal of Law, Tech. & Arts, (6), pp 1-25.

B. Custers, H. Ursic (2016), Big data and data reuse: a taxonomy of data reuse for balancing data benefits and personal data protection, in International Data Privacy Law, (6), p. 15-23.

A. Diker Vanberg, M.B. Ünver (2017), The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?, in European Journal of Law and Technology, (8), pp. 26-33.

P. Lee, K. Pickering (2016), The general data protection regulation: a myth-buster, in Journal of Data Protection & Privacy, pp-1-5.

H.T. Tavani, J.H. Moor (2000), Privacy Protection, Control of Information, and Privacy -Enhancing Technologies, in ACM SIGCAS Computers & Society, pp. 24-31.

Article 29 Data Protection Working Party (2017), Guidelines on Data Protection Impact Assessment (DPIA) and determining whther processing is "likely to result in a hight risk"

for the purposes of Regulation 2016/679.

Autori

Nadina Foggetti nadinafoggetti@gmail.com

Avvocato del Foro di Bari, mediatrice familiare e dottore di ricerca in Diritto Internazionale e dell'UE, ha conseguito un Master in Diritto Europeo e Transnazionale presso l'Università di Trento. Docente in corsi di perfezionamento e post-lauream, cultore della materia in Diritto Internazionale, Diritto dell'Unione Europea, del Commercio e Informatica Giuridica, attualmente ha un contratto per lo svolgimento dell'attività di ricerca presso l'Università degli studi di Bari "Aldo Moro" e ha partecipato a vari progetti nazionali e internazionali sui temi di cybercrime e cloud computing, nonchè sul diritto all'istruzione. Autrice di diversi articoli scientifici di carattere internazionale su varie tematiche tra cui gli aspetti giuridici collegati alle nuove tecnologie ICT. Fa parte di gruppi di lavoro internazionali sul tema della tutela delle persone con disabilità.