Corso di diritto pubblico di internet 2016/17

Privacy by design
Istituti e dinamiche nel nuovo regolamento europeo

(Simone Calzolaio)

Finalità dell'intervento

- descrivere la nuova strategia europea di protezione delle persone fisiche con riguardo alla protezione dei dati personali

Oggetto dell'intervento

- Le ragioni alla base del Reg. (Ue) 2016/679
- Introduzione al lessico della riforma
- La nozione di privacy by design (e di privacy by default)
- Istituti e dinamiche attuative della privacy by design

Corso di diritto pubblico di internet 2016/17

Le ragioni alla base del Reg. (Ue) 2016/679

Le ragioni: ***società ed economia digitale***

(cons. 6)

La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali.

La portata della **condivisione** e della **raccolta** di dati personali è aumentata in modo significativo.

La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività.

Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano.

La **tecnologia** ha trasformato l'**economia** e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali.

Corso di diritto pubblico di internet 2016/17

Le ragioni alla base del Reg. (Ue) 2016/679

I problemi da risolvere: ***frammentazione giuridica***

(cons. 9)

Sebbene i suoi obiettivi e principi rimangano tuttora validi, la direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche.

La compresenza di **diversi livelli di protezione** dei diritti e delle libertà delle persone fisiche, in particolare del diritto alla protezione dei dati personali, con riguardo al trattamento di tali dati negli Stati membri può ostacolare **la libera circolazione dei dati personali all'interno dell'Unione**.

Tali differenze possono pertanto costituire un freno all'esercizio delle **attività economiche su scala dell'Unione [ndr: Mercato unico digitale]**, falsare la concorrenza e impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione.

Tale divario creatosi nei livelli di protezione è dovuto alle divergenze nell'attuare e applicare **la direttiva 95/46/CE**

Cfr. D. Erdos, *European Data Protection Regulation and the New Media Internet: Mind the Implementation Gaps*, in «Legal studies research, Paper series», University of Cambridge, paper n. 30/2015 – in questo studio si dimostra che sussiste un divario rilevante all'interno dei singoli Stati nazionali europei nella protezione dei dati in riferimento alle nuove tecnologie.

Corso di diritto pubblico di internet
2016/17

Le ragioni alla base del Reg. (Ue) 2016/679

I problemi da risolvere:
oltre la tutela formale, uniforme e astratta

Si tratta di un aspetto che si coglie implicitamente comparando le forme di tutela apprestate nella direttiva 95/46/CE con le nuove forme di tutela apprestate nel Reg. (UE) 2016/679

Il modello di tutela attuale (fatto proprio anche dal Codice privacy, d.lgs. 196/2003) è improntato alla identificazione di alcune *nozioni base* (**dato personale, dato sensibile** ecc.) e poi ad una struttura *rigida e uniforme* di tutela fondata (essenzialmente) sul binomio **informativa**/**consenso**.

Soddisfatto il modello normativo – e cioè: una volta prestato il consenso all'informativa predisposta dal titolare/responsabile del trattamento – non viene richiesta alcuna particolare implementazione della struttura aziendale e aggiornamento dei modelli di tutela, protezione, sicurezza dei dati personali.

Si tratta di un modello di tutela pressoché unanimemente ritenuto non adeguato alla società ed economia digitale. Nella slide seguente cerco di spiegare (almeno) le principali ragioni di questa osservazione

Corso di diritto pubblico di internet 2016/17

Le ragioni alla base del Reg. (Ue) 2016/679

I problemi da risolvere:

oltre la tutela formale, uniforme e astratta

Attualmente è possibile trarre informazioni strettamente personali (cd. sensibili) su una o più persone fisiche semplicemente incrociando dati (né personali, né sensibili, sulla base della vigente normativa europea e italiana) e dati personali.

È il fenomeno dei cd. «Big data»: una mole infinita di dati, che viene prodotta ogni giorno dalla vita digitale di persone, imprese, amministrazioni, ed ogni giorno trattata e conservata (apparentemente) in quei non-luoghi chiamati cloud.

Questi dati, se correttamente interrogati, sono una fonte di informazioni infinita, e di una utilità ed un valore inedito nella storia dell'uomo.

Ne è nato un nuovo e fiorente settore di ricerca ed industriale: la «**big data analytics**».

Quel che interessa in questa sede puntualizzare è che attualmente per trarre informazioni analitiche su singole persone non è più necessario trattare dati personali o sensibili.

È sufficiente interrogare correttamente i big data e incrociare (**data inference** e **re-identification**) dati non personali per ottenere informazioni personali analitiche, intime, riservate.

Una spiegazione esaustiva del fenomeno e della possibilità tecnica – molto contestata nel dibattito internazionale – di farlo convivere con gli strumenti della privacy si trova in G. D'Acquisto, J. Domingo-Ferrer, P. Kikiras, V. Torra, Y. A. de Montjoye, A. Bourka, ***Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics***, European Union Agency for network and information security, december 2015, in <http://www.enisa.europa.eu>

Corso di diritto pubblico di internet
2016/17

Introduzione al lessico della riforma

Nuove definizioni (per nuova tutela)

Come ben si comprende, se si può facilmente dimostrare che le attuali forme di tutela non sono adeguate al fenomeno della protezione dei dati delle persone fisiche, ben più ardua si manifesta la ricerca di nuove forme di tutela efficaci.

A tal fine, si deve osservare che il Reg. UE procede ad identificare e definire nuovi vocaboli.

Fra questi, è necessario indicarne 3 e trattarne subito 2:

«**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per **valutare determinati aspetti personali** relativi a una persona fisica, in particolare **per analizzare o prevedere** aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

«**pseudonimizzazione**»:il trattamento dei dati personali in modo tale che i dati personali **non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive**, a condizione che tali informazioni aggiuntive siano **conservate separatamente** e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile

rischio del trattamento, rischio elevato, rischio per la sicurezza

Corso di diritto pubblico di internet 2016/17

Introduzione al lessico della riforma

Nuove definizioni (per nuova tutela)

Perché è così rilevante il tema della cd. «profilazione»?

(cfr. cons. 71 e art. 22 Reg. UE)

Perché il rischio concreto è che l'interessato possa veder leso il suo **diritto a non essere sottoposto a una decisione**, che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia **basata unicamente su un trattamento automatizzato** e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona, quali il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani.

Tale trattamento comprende la «profilazione».

Tuttavia, è consentito adottare decisioni sulla base di tale trattamento, compresa la profilazione, se ciò è:

a) espressamente previsto dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento, anche a fini di monitoraggio e prevenzione delle frodi e dell'evasione fiscale secondo i regolamenti, le norme e le raccomandazioni delle istituzioni dell'Unione o degli organismi nazionali di vigilanza e a garanzia della sicurezza e dell'affidabilità di un servizio fornito dal titolare del trattamento,

b) necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento,

c) o se l'interessato ha espresso il proprio consenso esplicito.

Corso di diritto pubblico di internet
2016/17

Introduzione al lessico della riforma

Nuove definizioni (per nuova tutela)

Perché è così rilevante il tema della cd. «profilazione»?

(cfr. cons. 71 e art. 22 Reg. UE)

In ogni caso, tale trattamento (automatizzato) dovrebbe essere subordinato a **garanzie adeguate**, che dovrebbero comprendere:

- la specifica informazione all'interessato;
- il diritto di ottenere l'intervento umano;
- di esprimere la propria opinione;
- di ottenere una spiegazione della decisione conseguita dopo tale valutazione;
- di contestare la decisione.

Tale misura non dovrebbe riguardare un minore.

Corso di diritto pubblico di internet
2016/17

Introduzione al lessico della riforma

Nuove definizioni (per nuova tutela)

Perché è così rilevante il tema della cd. «profilazione»?

(cfr. cons. 71 e art. 22 Reg. UE)

Di seguito si cita la seconda parte del cons. 71, perché a partire dall'analisi del problema della profilazione e del processo decisionale automatizzato lascia emergere i caratteri principali della nuova forma di tutela che chiamiamo **privacy by design**.

Al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le **circostanze** e il **contesto specifici** in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche **appropriate** per la profilazione, metta in atto **misure tecniche e organizzative adeguate** al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia **minimizzato il rischio** di errori e al fine di **garantire la sicurezza** dei dati personali secondo una modalità che tenga conto dei **potenziali rischi esistenti** per gli interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti.

Corso di diritto pubblico di internet
2016/17

La nozione di
privacy by design
e di
privacy by default

Come garantire una tutela così complessa per trattamenti così diversificati e potenzialmente non determinabili a priori?
(cfr. cons. 78 e art. 25 Reg UE)

Art. 25

Protezione dei dati fin dalla progettazione [privacy *by design*]

1.Tenendo conto dello **stato dell'arte** e dei **costi di attuazione**, nonché della **natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento**, come anche dei **rischi** aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, **sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento** stesso il titolare del trattamento mette in atto **misure tecniche e organizzative adeguate**, quali la **pseudonimizzazione**, volte ad attuare in modo efficace i principi di protezione dei dati, quali la **minimizzazione**, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

Corso di diritto pubblico di internet
2016/17

La nozione di privacy by design e di privacy by default

Come garantire una tutela così complessa per trattamenti così diversificati e potenzialmente non determinabili a priori?

(cfr. cons. 78 e art. 25 Reg UE)

Art. 25

Protezione dei dati per impostazione predefinita [*by default*]

2. Il titolare del trattamento mette in atto **misure tecniche e organizzative adeguate** per garantire che siano trattati, per **impostazione predefinita**, **solo i dati personali necessari per ogni specifica finalità del trattamento**. Tale obbligo vale per la **quantità** dei dati personali raccolti, la **portata** del trattamento, il **periodo di conservazione** e l'**accessibilità**. In particolare, **dette misure garantiscono che**, per impostazione predefinita, **non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica**.

3. Un **meccanismo di certificazione** approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per **dimostrare** la conformità ai requisiti di cui ai **paragrafi 1 e 2** del presente articolo.

Corso di diritto pubblico di internet
2016/17

La nozione di privacy by design e di privacy by default

Come garantire una tutela così complessa per trattamenti così diversificati e potenzialmente non determinabili a priori?

(cfr. cons. 78 e art. 25 Reg UE)

La "logica" della privacy by design e by default

… Dal rispetto del "modello" …

La responsabilità del titolare/responsabile del trattamento non si valuta (più) sul rispetto di norme cogenti astratte, che fissano concetti e nozioni predeterminate (soggette a rapida obsolescenza).

… alla promozione di una dinamica …

La responsabilità del titolare/responsabile del trattamento si valuta sulla messa in opera di **misure tecniche e organizzative adeguate**, fondata sulla premessa che:

- il titolare/responsabile del trattamento conosce [è tenuto a conoscere] nel dettaglio i rischi immediati, potenziali, progressivi dei trattamenti di dati personali posti in essere;
- il titolare/responsabile del trattamento è il soggetto cui deve essere affidata la responsabilità di una struttura aziendale in grado di garantire in concreto i diritti dell'interessato;
- Il titolare/responsabile del trattamento deve garantire che i processi aziendali siano continuamente aggiornati e adeguati ai trattamenti via via svolti.
- … estensione anche al settore degli appalti pubblici

Corso di diritto pubblico di internet
2016/17

Istituti e dinamiche attuative della privacy by design

Panoramica dei principali istituti e delle dinamiche connesse con la privacy by design

Un primo aspetto su cui mi sembra decisivo convogliare l'attenzione è il rilievo che il Reg. UE riconosce al tema del "rischio" ed il suo stretto legame con la dinamica della privacy by design e by default.

Il cons. 76 afferma che La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla **natura, all'ambito di applicazione, al contesto e alle finalità del trattamento**. Il rischio dovrebbe essere considerato in base a una **valutazione oggettiva** mediante cui si stabilisce se i trattamenti di dati comportano un **rischio** o un **rischio elevato**.

Il cons. 77 afferma che per dimostrare la **conformità** da parte del titolare del trattamento/responsabile del trattamento è necessario attenersi ai **codici di condotta approvati** e/o **alle certificazioni approvate** e/o **linee guida fornite dal comitato** e/o **indicazioni fornite da un responsabile della protezione dei dati**.

Il cons. 83 aggiunge che Per mantenere la **sicurezza** e **prevenire** trattamenti in **violazione** al presente regolamento, il titolare/responsabile del trattamento dovrebbe **valutare i rischi** inerenti al trattamento e attuare misure per limitare tali rischi, quali la **cifratura**.

Istituti e dinamiche attuative della privacy by design

Il primo elemento caratteristico della privacy by design è pertanto la valutazione sistematica da parte del titolare/responsabile del trattamento dei rischi attuali e potenziali del trattamento, sia in riferimento alla protezione dei diritti dell'interessato sia in riferimento specifico alla sicurezza dei dati.

La valutazione del rischio non è rimessa alla mera sensibilità dell'interessato ma trova una oggettivazione (dinamica) nella **conformità** della valutazione ai **codici di condotta approvati** e/o **alle certificazioni approvate** e/o **linee guida fornite dal comitato** e/o **indicazioni fornite da un responsabile della protezione dei dati.**

Corso di diritto pubblico di internet
2016/17

Istituti e dinamiche attuative della privacy by design

Panoramica dei principali istituti e delle dinamiche connesse con la privacy by design

E' nel quadro della valutazione e gestione del rischio del trattamento che possono essere introdotti due nuovi istituti del Reg. Ue.

La valutazione di impatto privacy (cons. 84 e art. 35)

Qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche (come avviene di norma per i **trattamenti che prevedono l'uso delle nuove tecnologie**), il titolare del trattamento dovrebbe essere responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per individuare, valutare e gestire il rischio.

L'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento.

Laddove la valutazione d'impatto sulla protezione dei dati indichi che i trattamenti presentano un rischio elevato che il titolare del trattamento non può attenuare mediante misure opportune in termini di tecnologia disponibile e costi di attuazione, **prima del trattamento si dovrebbe consultare l'autorità di controllo**.

Corso di diritto pubblico di internet
2016/17

Istituti e dinamiche attuative della privacy by design

Panoramica dei principali istituti e delle dinamiche connesse con la privacy by design

Il Responsabile per la protezione dei dati personali (art. 37)

Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure

c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

5.Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.

Corso di diritto pubblico di internet 2016/17

Istituti e dinamiche attuative della privacy by design

Panoramica dei principali istituti e delle dinamiche connesse con la privacy by design

Il Responsabile per la protezione dei dati personali (art. 37)

6.Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi. 7.Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.

Ai sensi dell'art. 38 al responsabile della protezione dei dati deve essere garantita autonomia decisionale e funzionale

Corso di diritto pubblico di internet 2016/17

Istituti e dinamiche attuative della privacy by design

Panoramica dei principali istituti e delle dinamiche connesse con la privacy by design

Il Responsabile per la protezione dei dati personali (art. 37)

Ai sensi dell'art. 39 1.Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35; d) cooperare con l'autorità di controllo; e

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione. 2.Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.