UNIVERSITÀ DI TRENTO

DIPARTIMENTO
FACOLTÀ DI GIURISPRUDENZA

lawtech
The Law and Technology Research Group

Diritto comparato della privacy

Lezione 16 – Privacy by design

Università di Trento – Facoltà di Giurisprudenza
a.a. 2021-2022

Paolo Guarda, Giorgia Bincoletto

L’ordine del ragionamento

1. Le origini della privacy by design: un’analisi comparata

2. L’art. 25 del GDPR: data protection by design e by default

3. Un’applicazione in ambito di sanità elettronica

1. Le origini della privacy by design

- Diritto e tecnologia
- «Code is law» (Lessig, *Code*, 1999)
- Dagli anni 90': *Digital Rights Management* (DRM) per proteggere il copyright e *Privacy Enhancing Technologies* per la privacy

1. Le origini della privacy by design

Una definizione (Bincoletto, 2019)

«Il principio di privacy by design impone l'**incorporazione** delle regole e dei valori della privacy **fin dalla progettazione** dei prodotti e dei servizi».

«Ridefinire la privacy alla luce di questa metodologia comporta che essa non sia più solo un diritto spettante ad un soggetto *ex post*, ma che abbia in sé la pretesa di essere tutelato *ex ante* fin dalla progettazione del bene o servizio».

1. Le origini della privacy by design: Canada

Principi (Cavoukian, 2009)

1. Proactive not reactive, Preventative not remedial
2. Privacy as the Default Setting
3. Privacy Embedded into design
4. Full functionality – Positive-sum, Not zero-sum
5. End-to-end security – Full lifecycle protection
6. Visibility and transparency – Keep it Open
7. Respect for User Privacy – Keep it User-Centric

1. Le origini della privacy by design: Canada

Office of the Privacy Commissioner of Canada (OPC) vs. Google Street:

- rilevazione fotografica
- raccolta delle informazioni anche da abitazioni di privati dotati di rete wireless non protetta
- reclamo contro Google lamentando le seguenti violazioni della PIPEDA: la raccolta dei dati non è stata limitata a quanto necessario agli scopi identificati dall'organizzazione; la raccolta è stata operata senza una previa definizione e una dichiarazione degli scopi; la raccolta è avvenuta senza che gli individui ne fossero a conoscenza o che potessero esprimere il loro consenso
- Secondo OPC, le violazioni potevano essere evitate dalla preventiva predisposizione di adeguate procedure e garanzie e da corrette privacy policies

Office of the Privacy Commissioner of Canada, *PIPEDA Case Summary #2011-001*

1. Le origini della privacy by design

- 32° International Conference of Data Protection and Privacy Commissioners, *Resolution on Privacy by design,* 27-29 ottobre 2010
- Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymaker*, FTC Report 2012
- Proposta di GDPR, COM/2012/011 final - 2012/0011

1. Le origini della privacy by design

Resolution on Privacy by design (2010)

1. Riconoscimento della Privacy by Design come “essential component of fundamental privacy protection”;
2. Adozione dei Privacy by Design’s Foundational Principles;
3. Impegno alla promozione dell’approccio a livello organizzativo, educativo e governativo

1. Le origini della privacy by design: US

«Each **covered entity** shall, in a manner **proportional** to the size, type, and nature of the covered information that it collects, implement a **comprehensive information privacy program** by:

(1) **incorporating necessary development processes and practices** throughout the product life cycle that are designed to safeguard the **personally identifiable information** that is covered information of individuals based on: (A) the **reasonable expectations of such individuals regarding privacy**; and (B) the relevant **threats** that need to be guarded against in meeting those expectations;

(2) maintaining appropriate **management** processes and practices throughout the data life cycle that are designed to ensure that information systems comply with: (A) the provisions of this Act; (B) the **privacy policies** of a covered entity; and (C) the privacy **preferences** of individuals that are consistent with the consent choices and related mechanisms of individual participation as described in section 202»

Sec. 103, Commercial Privacy Bill of Rights Act of 2011

1. Le origini della privacy by design: US

Federal Trade Commission vs. Google Buzz

«is further ordered that respondent, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a **comprehensive privacy program** that is reasonably **designed** to: (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information».

Federal Trade Commission, Google, Inc.; *Analysis of proposed consent order to aid public comment*, 76 Federal Register, April 5 2011

1. Le origini della privacy by design: US

«Companies should promote **consumer privacy** throughout their **organizations and at every stage of the development of their products and services**. The preliminary staff report called on companies to promote consumer privacy throughout their organizations and at every stage of the development of their products and services. Although many companies already incorporate substantive and procedural privacy protections into their business practices, industry should implement **privacy by design more systematically**».

Federal Trade Commission, Report, 2012

1. Le origini della privacy by design: US

- Code of Fair Information Practices (1973)
- OECD's Guidelines on the protection of privacy and transborder flows of personal data (1980, revisione nel 2013)
- American Law Institute, *ALI data privacy principles*, 2019

1. Le origini della privacy by design

Alcune criticità, in bilanciamento

- Flessibilità della norma giuridica vs. rigidità della tecnologia
- Interpretazione di principi e regole dell'operatore del diritto vs. autoregolazione del privato
- Bilanciamento dei diritti in sede giudiziaria vs. bilanciamento al momento dello sviluppo della tecnologia o pratica organizzativa
- Maggior protezione dei diritti e attenzione alla sicurezza dei dati vs maggiori costi in una società del capitalismo della sorveglianza

1. Le origini della privacy by design

Alcune potenzialità, in bilanciamento

- Principio tecnologicamente neutrale vs. obsolescenza tecnologica
- Approccio globale e da adottare *ex ante* vs. trovare una soluzione dopo che i dati personali sono stati violati (es. data breach)
- Aumento della fiducia nel prodotti e servizi vs. «asimmetria informativa»

2. L’art. 25 del GDPR

«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».

2. L’art. 25 del GDPR

CHI?

- «titolare del trattamento» (Art. 4, par. 1, n. 7 GDPR, v. Lezione 12)
- Responsabile del trattamento? Art. 28 par.1 supporto al titolare

Considerando 78: «In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, **i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati** a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati»

2. L’art. 25 del GDPR

COSA?

- mette in atto misure tecniche e organizzative
- adeguate, quali la pseudonimizzazione

2. L’art. 25 del GDPR

COSA?

- Definizione in Art. 4, par. 1, n 5) GDPR: «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».

2. L’art. 25 del GDPR

QUANDO?

- sia al momento di determinare i mezzi del trattamento
- sia all'atto del trattamento stesso

2. L’art. 25 del GDPR

COME? CRITERI

- 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

2. L’art. 25 del GDPR

PERCHÉ? FINE

- (misure) 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

2. L’art. 25 del GDPR

I principi di protezione dei dati, quali la minimizzazione

Art. 5 GDPR

- «liceità, correttezza e trasparenza»
- «limitazione della finalità»
- «minimizzazione dei dati»
- «esattezza»
- «limitazione della conservazione»
- «integrità e riservatezza»
- «responsabilizzazione»

2. L’art. 25 del GDPR

Data Protection 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».

2. L’art. 25 del GDPR e oltre

CERTIFICAZIONE (es. da International Standard Association, CE, organismi nazioni di accreditamento)

«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».

NORME COLLEGATE: Artt. 30, 32, 35, 83 GDPR

2. L’art. 25 del GDPR e oltre

- Art. 67, Regolamento (UE) 2017/1939 relativo all’attuazione di una cooperazione rafforzata sull’istituzione della Procura europea;
- Artt. 27 e 85, Regolamento (UE) 2018/1725 in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell’Unione;
- Art. 16, D.lgs. 18 maggio 2018, n. 51, emanato per l’attuazione della direttiva 2016/680 (law enforcement);
- Art. 2-*septiesdecies*, Codice Privacy.

3. Un’applicazione in ambito di sanità elettronica

- Approccio necessariamente interdisciplinare
- Tanti possibili ambiti applicativi (videosorveglianza, social networks, ecc.)
- La sanità elettronica

3. Un’applicazione in ambito di sanità elettronica

- Electronic Health Record e Personal Health Record
- Fascicolo sanitario elettronico (FSE) e cartella clinica del cittadino
- Telemedicina e *mHealth apps*

3. Un'applicazione in ambito di sanità elettronica

- Prima sanzione in assoluto con il GDPR
- Autorità garante portoghese sanziona per 400.00 euro un ospedale pubblico per mancata adozione di misure tecniche e organizzative nel sistema di accesso e autorizzazione ai dati clinici dei pazienti

3. Un’applicazione in ambito di sanità elettronica

- Electronic Health Record e data protection by design

- Lista di *technical and organisational guidelines* divise tra *data at rest, in use, in transit* e tra *before* e *during the processing*

Riferimenti bibliografici

- G. Bincoletto, *Data protection by design in the e-health care context: theoretical and applied perspectives*, Nomos, 2021 (in corso di pubblicazione)
- G. Bincoletto, “European Union · EDPB Guidelines 4/2019 on Data Protection by Design and by Default”. In: *EDPL* 6(4) (2020), pp. 574-579
- G. Bincoletto, *La privacy by design. Un’analisi comparata nell’era digitale*, Roma, Aracne Editrice, 2019
- A. Cavoukian, Privacy by design: The 7 foundational principles, 2009

Copyright