UNIVERSITÀ DI TRENTO

DIPARTIMENTO
FACOLTÀ DI GIURISPRUDENZA

lawtech
The Law and Technology Research Group

Diritto civile A-J

Lezione 17 – Privacy by design e privacy by default

Università di Trento – Facoltà di Giurisprudenza
a.a. 2020-2021

Roberto Caso, Giorgia Bincoletto

L’ordine del ragionamento

1. Le origini della privacy by design
2. L’art. 25 del GDPR: data protection by design e by default
3. Qualche ambito applicativo

1. Le origini della privacy by design

- Diritto e tecnologia: dall'invenzione della scrittura all'era digitale (Pascuzzi, 2020)
- Necessaria interdisciplinarietà dei problemi e delle soluzioni
- *Lex informatica* (Reidenberg, 1997) e *Code is law* (Lessig, 1999 e 2006)

1. Le origini della privacy by design

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

- 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 Regolamento del Parlamento Europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati). COM/2012/011 final - 2012/0011

1. Le origini della privacy by design

The 32nd International Conference of Data Protection and Privacy Commissioners gathered at Jerusalem therefore resolves to:

1. Recognize Privacy by Design as an essential component of fundamental privacy protection;

2. Encourage the adoption of Privacy by Design's Foundational Principles, such as those set out below as guidance to establishing privacy as an organization's default mode of operation;

3. Invite Data Protection and Privacy Commissioners/Authorities to:

   a. promote Privacy by Design, as widely as possible through distribution of materials, education and personal advocacy;
   b. foster the incorporation of the Privacy by Design Foundational Principles in the formulation of privacy policy and legislation within their respective jurisdictions;
   c. proactively encourage research on Privacy by Design;
   d. consider adding Privacy by Design to the agendas of events taking place on International Data Privacy Day (January 28);
   e. report back to the 33rd International Data Protection and Privacy Commissioners Conference, where appropriate, on Privacy by Design activities and initiatives undertaken within their jurisdictions with a view to sharing best practices.

1. Le origini della privacy by design

«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, 2012)

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

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?

- «La pseudonimizzazione infatti consiste nel sostituire un attributo, solitamente univoco, di un dato con un altro, ugualmente univoco e solitamente non immediatamente intellegibile». (Acquisto, G., & Naldi, M., 2017)

- 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

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 GDPR

3. Qualche ambito applicativo (?)

- https://www.facebook.com/business/news/facebooks-commitment-to-data-protection-and-privacy-in-compliance-with-the-gdpr

- https://privacy.google.com/businesses/compliance/

- https://www.amazon.it/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ: «Secure Sockets Layer (SSL), che cripta le informazioni che fornisci. Rispettiamo gli standard di sicurezza Payment Card Industry Data Security Standard (PCI DSS)»

3. Qualche ambito applicativo

- Ambito sanitario (es. fascicolo sanitario elettronico)

- Ambito della videosorveglianza (es. schermatura dei volti prima dell'autorizzazione all'utilizzo del video)

- Ad. es., come vedremo alla lezione 19 sul contrasto alla pandemia, l'app IMMUNI indica di seguire il principio di data protection by design

Riferimenti bibliografici

- G. Bincoletto, La privacy by design. Un'analisi comparata nell'era digitale, Roma, Aracne Editrice, 2019
- G. Pascuzzi, Il diritto dell'era digitale, Bologna, Il Mulino, 2020, pp. 77-111
- A. Cavoukian, Privacy by design: The 7 foundational principles, 2009
- L. Lessig, Code. 2.0. New York, Basic Books, 2006
- J. R. Reidenberg, "Lex informatica: The formulation of information policy rules through technology". In: Tex. L. Rev. 76 (1997), pp. 553–593.

Roberto Caso, Giorgia Bincoletto

E-mail:
roberto.caso@unitn.it
giorgia.bincoletto@unitn.it

Web:
http://www5.unitn.it/People/it/Web/Persona/PER0000633#INFO
http://lawtech.jus.unitn.it/
https://www.robertocaso.it/

Copyright