assonime

Associazione fra le società italiane per azioni

3/2020

Interventi

III Conferenza Nazionale Cybersecurity e Privacy

Cybersecurity e protezione dei dati: rischi e danni nella prospettiva della trasformazione digitale

Alcuni spunti di riflessione

Ginevra Bruzzone

Università degli Studi di Roma Tor Vergata

20 gennaio 2020

Outline

1. Sicurezza nel contesto della trasformazione digitale
2. Le tipologie di danno in un mondo interconnesso
3. Un focus sui rischi di azioni risarcitorie
4. Lo spazio di scelta per le imprese
5. Gli ambiti dell'intervento pubblico

1

1

1. Sicurezza nel contesto della trasformazione digitale

- la trasformazione digitale pone importanti sfide sul piano della sicurezza, tra cui quelle della cybersecurity e della protezione dei dati personali: occorre che il quadro giuridico, europeo e nazionale, sia adeguato
- guardando in parallelo al quadro giuridico per la protezione dei dati personali e alla disciplina europea e nazionale della cybersecurity (su cui cfr. circolare Assonime n. 30/2019), emergono alcune caratteristiche comuni
- quali sono le questioni aperte per quanto riguarda gli spazi di scelta per le imprese e il ruolo della politica pubblica?

2

2

2. Le tipologie di danno in un mondo interconnesso

- la trasformazione digitale porta verso un mondo sempre più interconnesso (internet of things, intelligenza artificiale e così via), in cui per definizione aumenta l'esposizione a rischi di violazione dei dati personali e a rischi cyber (non solo attacchi, anche disfunzioni)
- è ampia la varietà dei pregiudizi che ne possono derivare: danni economici; danni fisici; danni immateriali alla persona (ad es. perdita riservatezza, danno alla reputazione); danni con una dimensione politico/sociale
- danni per l'ente che subisce l'incidente e danni per soggetti terzi, che possono ripercuotersi sull'ente, in termini di reputazione e se deve ripristinare/risarcire
- sia la disciplina NIS che il GDPR indicano criteri oggettivi per stabilire la probabilità e la gravità dei rischi, con riguardo ad esempio all'attività, alla dipendenza da reti, servizi e sistemi ICT, alla natura, al contesto e alle finalità dei trattamenti di dati personali

3

3

3. Un focus sul rischio di azioni risarcitorie

4

4

Rischio di azioni risarcitorie per danni a terzi

- per la violazione delle norme a tutela dei dati personali si sta già diffondendo in vari Stati dell'Unione europea un contenzioso di natura risarcitoria
- tradizionalmente, come indicato anche da pronunce recenti della Cassazione (Cass. 3426/2018) il focus delle azioni risarcitorie era sulla tutela della vita privata e della riservatezza => diritto al risarcimento di un danno nella sfera non patrimoniale di interessi del danneggiato (Cass. 18812/2014). Valevano quindi le indicazioni fornite dalle Sezioni Unite della Cassazione n. 26972/2008 sul danno non patrimoniale, per cui la lesione deve essere seria (non futile o irrisoria) e il danno deve essere grave e dunque eccedere una certa soglia minima . Questi requisiti sono richiamati in varie pronunce della Cassazione che riguardano specificamente il danno non patrimoniale nel caso di violazioni privacy (v. Cass. 16133/2014 e anche Cass. 3311/2017)

5

5

Il danno da perdita di controllo sui dati

- con il GDPR il focus si amplia alla tutela del controllo sui propri dati, incluso il diritto alla portabilità => apertura, in un certo senso, a una visione anche economico/concorrenziale del dato personale
- in alcuni Stati membri i giudici hanno già riconosciuto risarcimenti in casi individuali di lesione del diritto alla tutela dei dati inteso come (mero) diritto a controllare i propri dati personali
- se il danno risarcibile si estende alla sfera «economica» e quindi del danno patrimoniale, la soglia di significatività del danno per l'azione risarcitoria viene ad abbassarsi
- nella misura in cui è più facile sostenere che i danni da perdita di controllo sono omogenei rispetto allo scenario del danno immateriale o da ansia/stress, aumenta il rischio di azioni collettive risarcitorie (stand alone o follow-on). V. casi in UK e Francia

6

6

Minimizzare il rischio di azioni risarcitorie

Impegnarsi nella prevenzione è importante per limitare i danni, all'ente e ai terzi, il rischio di sanzioni e anche il rischio di azioni risarcitorie

- in base al GDPR se c'è violazione della normativa sulla protezione dei dati personali e nesso di causalità, il titolare non può addurre considerazioni relative alla mancanza dell'elemento soggettivo per evitare il risarcimento (art. 82). Questo può essere evitato solo dimostrando che l'evento dannoso non gli è in alcun modo imputabile
- rispetto alle misure preventive, la Corte di Giustizia in *Google Spain* indica che nel contesto digitale gli obblighi vanno declinati in relazione al ruolo, alle responsabilità e alla situazione concreta del titolare del trattamento. Standard e certificazioni del livello di sicurezza possono svolgere un ruolo per dimostrare che l'impegno del titolare del trattamento è sufficiente a evitare violazioni della normativa
- analoghe considerazioni possono valere per i danni derivanti da violazione della normativa sulla cybersecurity

7

7

4. Lo spazio di scelta delle imprese

- per la prevenzione e la gestione dei rischi, il GDPR richiede la *data protection by default* e *by design*: questi principi si riflettono in tutta l'impostazione della normativa (considerando 78, art. 25)
- la *cybersecurity by design*, pur non essendo richiesta a livello normativo con un'analoga formulazione, è un approccio di fatto necessario
- per tradurre i principi di *data protection* e *cybersecurity by design* in scelte operative, occorrono investimenti tecnologici e scelte organizzative; quanto e come dipende dal contesto, occorre un'analisi costi/benefici – che richiede a sua volta la mappatura il più possibile completa dei rischi
- per un approccio simile al di fuori del contesto europeo, cfr. Sedona Conference 'Incident Response Guide', gennaio 2020

8

8

5. Gli ambiti dell'intervento pubblico

- Tenendo conto degli effetti esterni che possono derivare da violazioni della tutela dei dati personali e da attacchi cyber e più in generale dai rischi per la sicurezza connessi alla trasformazione digitale, la politica pubblica delinea un quadro generale entro cui vengono a collocarsi le scelte dei singoli

- Quattro principali ambiti di intervento:

a. fissazione di obblighi di condotta

b. governance pubblica per il monitoraggio e la gestione dei rischi e delle violazioni

c. promozione degli standard e dell'interoperabilità

d. requisito del controllo da parte dell'uomo - human oversight

9

9

a. Obblighi di condotta

- Obblighi che la normativa europea e nazionale pone in capo ai singoli enti. Cfr. ad esempio:

• obblighi per i titolari del trattamento previsti dal GDPR (DPO, registro trattamenti, valutazione di impatto; notifica dei data breach ecc.)

• obblighi per gli operatori di servizi essenziali nella disciplina NIS (misure di sicurezza, notifica degli incidenti)

• obblighi per i soggetti rientranti nel perimetro della sicurezza nazionale cibernetica

Anche per l'intelligenza artificiale si stanno ipotizzando a livello europeo *mandatory risk based requirements* per le applicazioni che comportano un elevato rischio

- **Le sfide per il legislatore**:

• mantenere obblighi proporzionati

• assicurare il coordinamento tra gli obblighi derivanti da diverse normative (ad es. NIS v. perimetro della sicurezza nazionale cyber)

10

10

b. Governance pubblica

- creazione dell'assetto organizzativo per il monitoraggio e la gestione delle violazioni, integrato a livello europeo e internazionale
- a livello europeo negli ultimi anni sono state ridisegnate l'architettura istituzionale per la tutela dei dati personali (con il GDPR) e quella della cybersecurity (con la direttiva NIS e il Cybersecurity Act, che ha rafforzato il ruolo dell'ENISA)
- analoghe iniziative, in parte derivanti dalla necessità di adeguarsi al quadro europeo, sono state assunte a livello nazionale
- **sfide aperte**: necessità che il sistema, anche sul fronte cyber, diventi presto pienamente operativo e funzioni in modo integrato. Il timore, soprattutto a livello nazionale, è che i cambiamenti troppo frequenti di governance e la molteplicità dei soggetti coinvolti possano finire per indebolire le capacità di vigilanza

11

11

c. Standardizzazione e interoperabilità

- promuovere la standardizzazione e l'interoperabilità delle soluzioni sul fronte della sicurezza nel contesto della trasformazione digitale rientra tra i principali compiti delle istituzioni europee nell'ambito della Digital Single Market Strategy
- il rispetto degli standard comporta la presunzione di conformità agli obblighi previsti dalla normativa europea
- la standardizzazione accompagnata dalla certificazione europea può svolgere un ruolo centrale di semplificazione del sistema, favorendo gli scambi e l'integrazione tra soggetti operanti in diversi paesi
- **le sfide attuali**: il Cybersecurity Act chiede alla Commissione di preparare un piano di azione entro giugno 2020 per avviare il sistema di certificazione europea della cybersecurity per reti, servizi e sistemi. Occorre definire l'ordine di priorità

12

12

d. Human oversight (i)

Un ulteriore modalità di intervento, rispetto ai rischi della trasformazione digitale, consiste nel porre limiti, in alcuni ambiti, alla gestione completamente automatizzata senza controllo umano

- nel trattamento dei dati personali il principio è consolidato. L'art. 22 GDPR prevede che l'interessato ha diritto a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. Eccezioni: se la decisione è necessaria per la conclusione o esecuzione di un contratto, se è autorizzata con adeguate garanzie dal diritto dell'Unione o di uno Stato membro o se è basata sul consenso esplicito (nel primo e nel terzo caso l'interessato ha comunque diritto di ottenere l'intervento umano e di contestare la decisione automatizzata)

13

13

d. Human oversight (ii)

- un'analoga esigenza si pone, a prescindere dalla tutela dei dati personali, rispetto a quei processi decisionali automatizzati che possono produrre gravi conseguenze, di varia natura (ad esempio, veicoli a guida autonoma). Tema rilevante per la strategia europea sull'intelligenza artificiale al servizio dell'uomo. I rischi possono derivare dal disegno del processo automatizzato, dalla scarsa qualità dei dati o dal processo di machine learning
- l'innovazione può contribuire a ottimizzare le capacità di controllo e quindi, nel tempo, a spostare la frontiera di quanto si può realizzare attraverso le macchine, consentendo così di aumentare le potenzialità che, nei vari settori, derivano dalle nuove tecnologie. In base al principio di precauzione, tuttavia, occorre interrogarsi in ogni ambito sulle modalità più efficaci per conseguire un sufficiente livello di sicurezza, utilizzando tutti gli strumenti a disposizione (prevenzione del rischio, gestione dell'incidente, livello del controllo da parte dell'uomo sui processi decisionali automatizzati)

14

14