III Conferenza Nazionale Privacy e Cybersecurity

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

Alcuni spunti di riflessione

Ginevra Bruzzone

Tor Vergata, 20 gennaio 2020

Spunti di riflessione

- il tema da discutere è ampio:
  - cybersecurity + protezione dei dati personali
  - rischi e danni nella prospettiva della trasformazione digitale
- proviamo a delineare in modo schematico il quadro di riferimento generale per proporre su questa base alcuni spunti e interrogativi per la successiva discussione
- guardiamo in parallelo al GDPR e alla disciplina della cybersecurity (direttiva 2016/1148/UE e d.lgs. n. 65/2018 – *disciplina NIS*; regolamento (UE) 2019/881 - *Cybersecurity Act*; d.l. 105/2019, convertito dalla legge n. 133/2019 – *perimetro della sicurezza nazionale cibernetica*; per una sintesi, cfr. circolare Assonime n. 30/2019)

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 cyber (non solo attacchi, anche disfunzioni) e la varietà dei pregiudizi che ne possono derivare
- varie tipologie di danni: danni economici; danni fisici; danni immateriali alla persona (ad es. perdita riservatezza, danno alla reputazione); danni con una dimensione politico/sociale
- danni diretti per l'ente che subisce l'incidente o danni per soggetti terzi (che possono portare a danni indiretti per l'ente, in termini di reputazione e se deve ripristinare/risarcire)
- sia il GDPR che la disciplina NIS indicano criteri oggettivi per stabilire la probabilità e la gravità dei rischi , con riguardo all'attività, alla dipendenza da reti, servizi e sistemi ICT, alla natura, al contesto e alle finalità dei trattamenti di dati personali

Rischio di azioni risarcitorie per danni a terzi

- Per la violazione delle norme a tutela dei dati personali si sta diffondendo in vari Stati dell'Unione un contenzioso di natura risarcitoria
- Tradizionalmente, come indicato anche da pronunce recenti della Cassazione (Cass. 3426/2018) il focus era sulla tutela della vita privata e della riservatezza e veniva riconosciuto il 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 peraltro 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)

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 già pronunce giurisprudenziali che hanno 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

Evitare l'imputabilità del danno

Lavorare sul fronte della prevenzione – anzitutto per ridurre i rischi e i danni, ma anche per ridurre il coinvolgimento nell'evento che genera il danno a terzi -nesso di causalità, imputabilità

- In base al GDPR, se 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, come accertare che l'impegno sia sufficiente a evitare la violazione del GDPR? Nel contesto digitale, come sottolineato dalla Corte di Giustizia nel caso *Google Spain*, gli obblighi vanno declinati in relazione al ruolo, alle responsabilità e alla situazione concreta del titolare del trattamento. Quale ruolo può essere svolto da standard e certificazioni del livello di sicurezza?
- Scenari del danno da violazione della normativa sulla cybersecurity; danno senza violazione della normativa

Data protection e cybersecurity by design: le valutazioni delle imprese

- Per la prevenzione e la gestione dei rischi, la data protection by default e by design è richiesta dal GDPR e si riflette in tutta la sua impostazione (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 questi approcci in scelte operative, occorrono investimenti tecnologici e scelte organizzative; quanto e come dipende dal contesto, analisi costi/benefici – che richiede a sua volta la mappatura il più possibile completa dei rischi. Impostazione che vale a prescindere dal contesto normativo (v. ad esempio in contesto US la recentissima Sedona Conference 'Incident Response Guide' del gennaio 2020)

I livelli dell'intervento pubblico

•L'ordinamento, tuttavia, non delega del tutto le scelte ai singoli soggetti. Siccome la solidità e la resilienza del sistema dipende da quella del livello più debole della catena, vi sono interventi di sistema che creano il quadro generale entro cui vengono a collocarsi le scelte dei singoli:

a. Obblighi di condotta

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

c. Standardizzazione

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

a. Obblighi di condotta

- Obblighi che, tenendo conto degli effetti esterni delle violazioni, la normativa europea e nazionale pone in capo ai singoli enti. Ad esempio:

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

• gli obblighi per gli operatori di servizi essenziali nella disciplina NIS – misure organizzative e di sicurezza, notifica degli incidenti

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

• si ipotizzando mandatory risk based requirements anche per high risk applications of AI

- La sfida per il legislatore è quella di mantenere obblighi proporzionati e di assicurare il coordinamento tra gli obblighi che discendono dalle diverse normative (ad es. NIS v. perimetro)

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, assunte a livello nazionale

→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

c. Standardizzazione

- Il terzo livello su cui interviene la politica pubblica è quello della standardizzazione dei livelli di sicurezza. Questo fronte, insieme a quello della certificazione europea, può svolgere un ruolo centrale di semplificazione del sistema, favorendo gli scambi e l'integrazione tra soggetti operanti in diversi paesi: uno dei fronti più importanti, oggi, della Digital Single Market Strategy. A che punto siamo sul fronte della standardizzazione e della certificazione della sicurezza?
- 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, secondo un ordine di priorità. Come in generale nell'utilizzo degli standard europei, potranno essere usati per presunzione di conformità a obblighi previsti dalla normativa europea

d. Human oversight

Sempre nell'ottica dell'intervento pubblico rispetto ai rischi della trasformazione digitale, ipotesi in cui per motivi diversi l'ordinamento non consente la gestione completamente automatizzata, senza controllo umano

- Nel trattamento dei dati personali art. 22 GDPR: 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. Non si applica se decisione necessaria per la conclusione o esecuzione di un contratto, autorizzata con adeguate garanzie dal diritto dell'Unione o di uno Stato membro o basata sul consenso esplicito (nel 1° e 3° caso il titolare deve consentire diritto a ottenere l'intervento umano, esprimere opinione e contestare decisione)

d. Human oversight (ii)

- Esigenze, sul fronte della sicurezza, anche a prescindere dalla tutela dei dati personali (es. veicoli a guida autonoma, medicina ecc.) L'approccio può essere diverso per alcune applicazioni ai processi di automazione in ambito industriale. Tema rilevante per la strategia europea sull'intelligenza artificiale al servizio dell'uomo. Rischi possono derivare da problemi nel disegno della tecnologia, 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, ci derivano dalle nuove tecnologie. Il principio di precauzione, tuttavia, ci chiederà in ogni caso e in ogni ambito di interrogarci sulle modalità più efficaci per conseguire sufficiente sicurezza, richiedendo in alcuni ambiti il controllo da parte dell'uomo o la possibilità di revisione umana della decisione automatizzata anche per il trattamento di dati non personali