La sicurezza dei dati nel trattamento dei dati personali

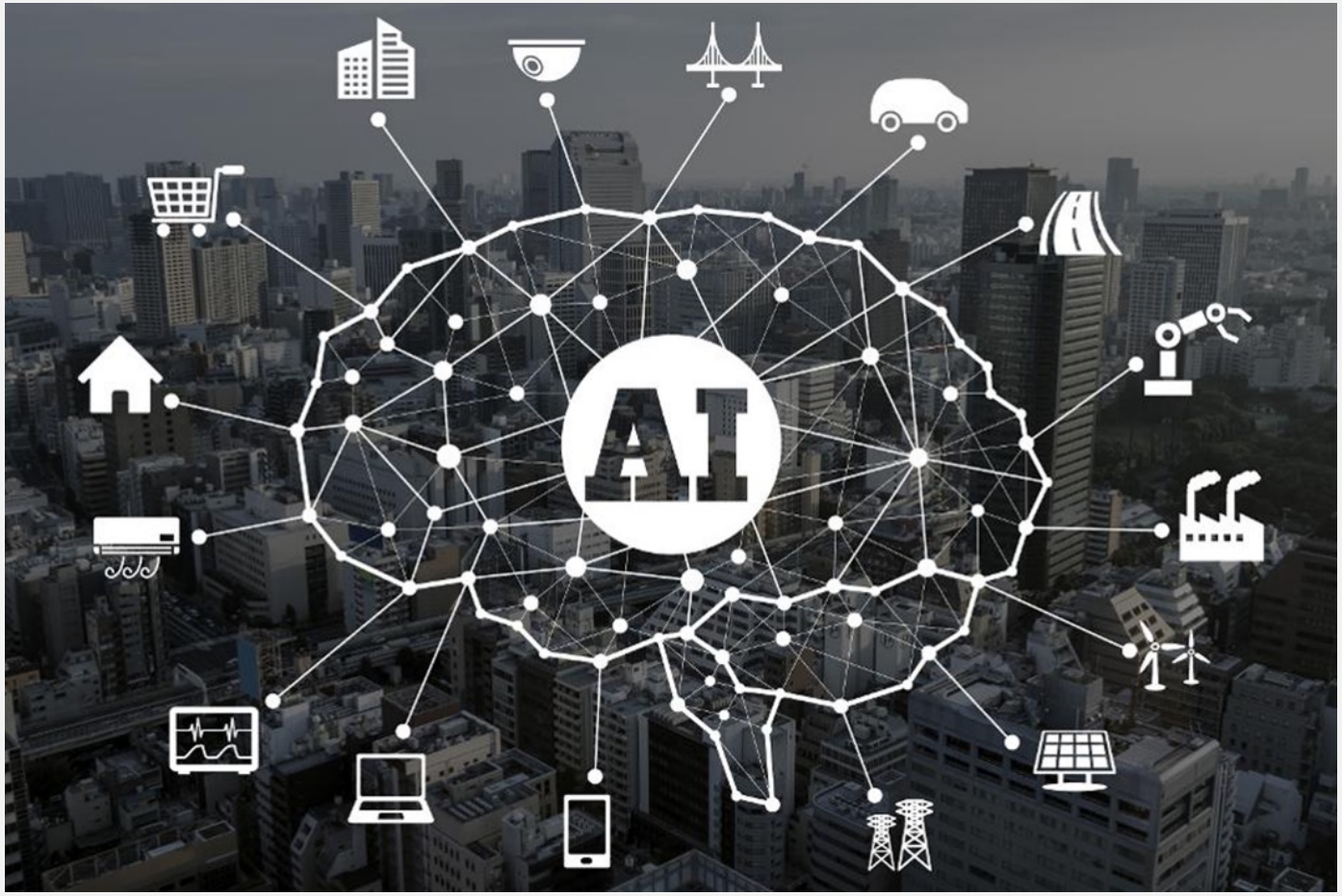
UNIVERSITÀ DEGLI STUDI DI MILANO

Big Data

Ubiquità

UNIVERSITÀ DEGLI STUDI DI MILANO

Algocrazia

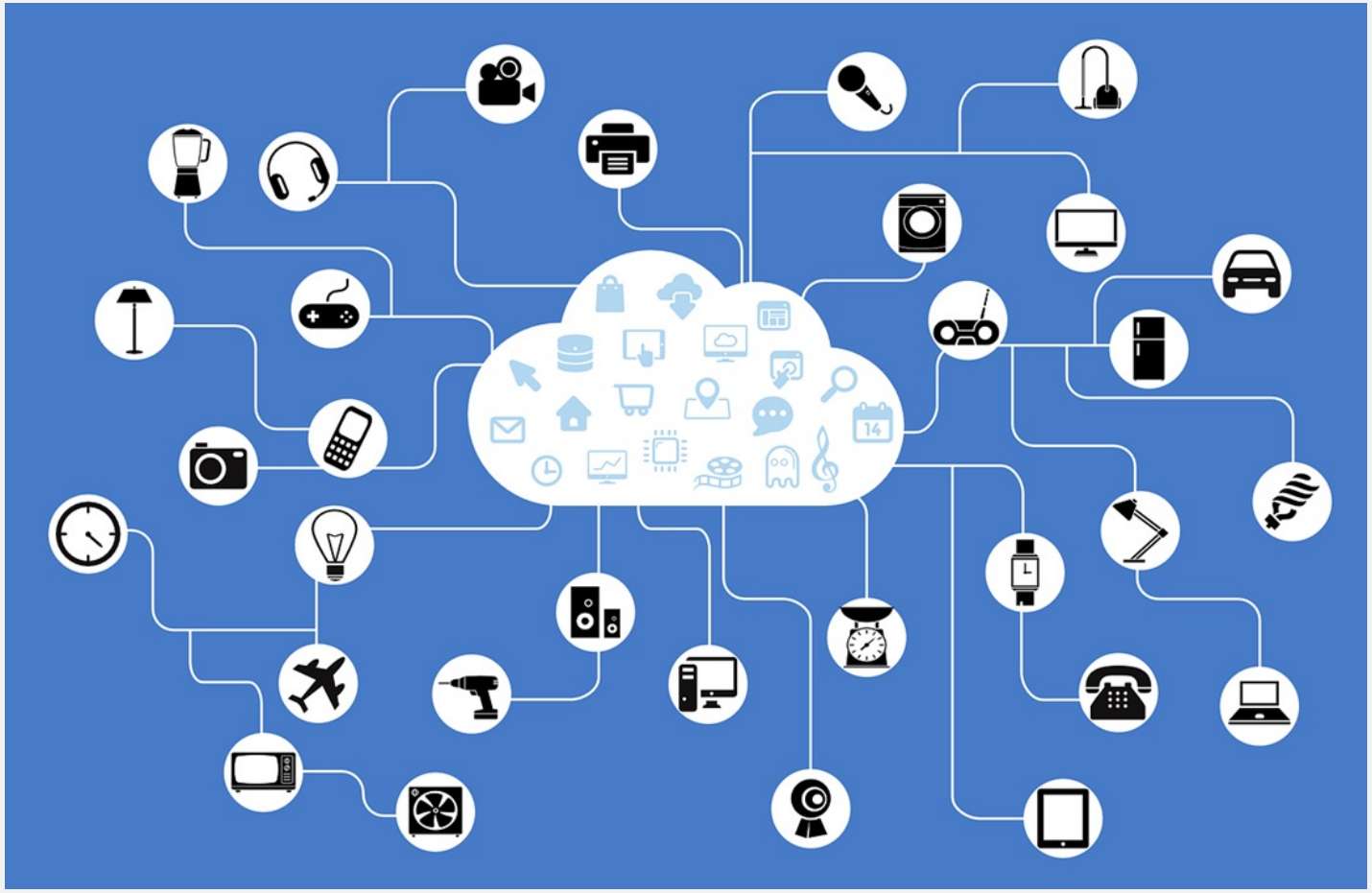


UNIVERSITÀ DEGLI STUDI DI MILANO

Profilazione

UNIVERSITÀ DEGLI STUDI DI MILANO

Sensor society



UNIVERSITÀ DEGLI STUDI DI MILANO

Minacce

UNIVERSITÀ DEGLI STUDI DI MILANO

Attacchi

Fonte: https://www.ispionline.it/it/pubblicazione/la-pandemia-ed-virus-20-25726

UNIVERSITÀ DEGLI STUDI DI MILANO

Data breach

Banking & Financial Services

Equifax says data breach has cost it nearly $2 billion so far

Email | Share | Share | Tweet | Save | Print | Order Reprints | Unlock Article

UNIVERSITÀ DEGLI STUDI DI MILANO

Ransomware

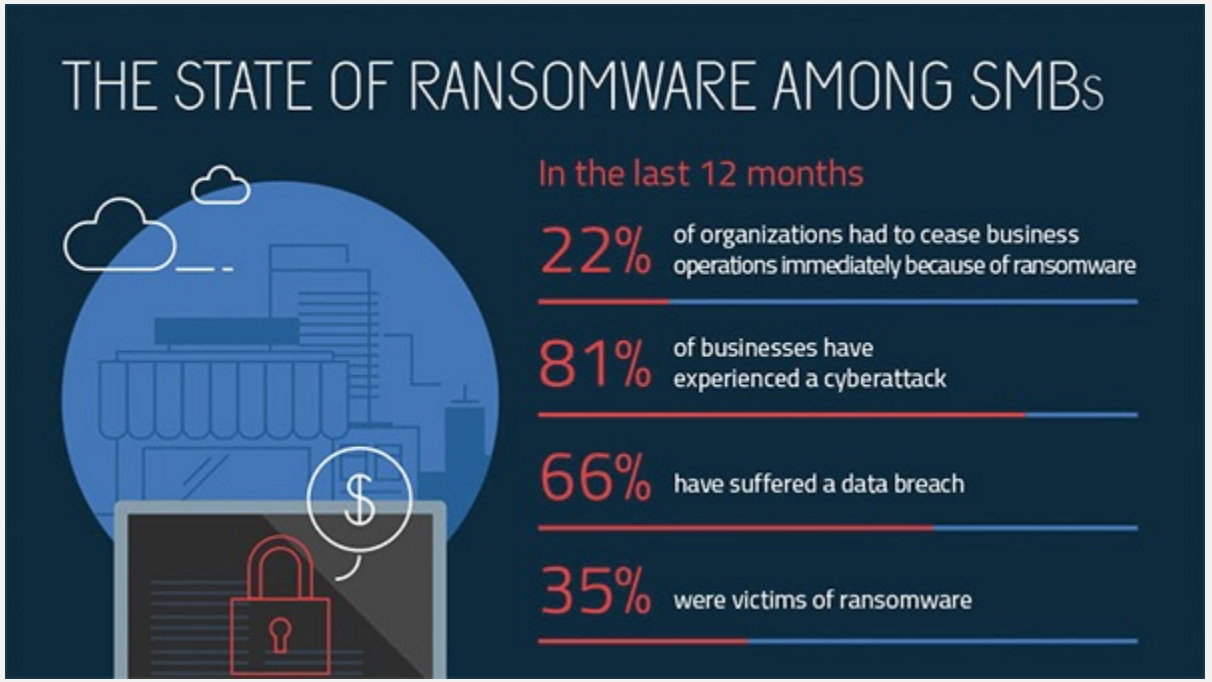
5,5mila

Attacco hacker mondiale: virus "Wannacry" chiede il riscatto, ospedali britannici in tilt. "Usato codice Nsa"

Un "ransomware" lanciato su centomila sistemi in 105 Paesi. Chiede soldi in Bitcoin, incognita l'origine. Pagamenti in corso, rischio truffa. Colpita anche l'Italia

UNIVERSITÀ DEGLI STUDI DI MILANO

Statistiche



UNIVERSITÀ DEGLI STUDI DI MILANO

OSINT

WIRED .IT Sezioni Gallery Wired Next

HOT TOPIC VACCINI D'ITALIA ESTATE TRAILER PRIDE FACEBOOK GOVERNO APPLE VIDEOGAME CHERNOBYL INTERNET... VEDI TUTTI

HOME INTERNET REGOLE

di **Raffaele Angius**
Contributor
24 JUN, 2019

1537

1537
CONDIVISIONI

Il ministero della Giustizia sta condividendo online i dati personali di migliaia di persone

Sul pvp, portale delle vendite pubbliche, sono caricati documenti non anonimizzati. Così le informazioni di migliaia di debitori sono disponibili in rete, anche con una banale ricerca su Google

Conseguenze

Considerando n. 85

"Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata".

UNIVERSITÀ DEGLI STUDI DI MILANO

I mantra dell'information security

- La sicurezza è un processo e non un prodotto.
- La sicurezza assoluta non esiste, ma è un processo asintotico.
- Be paranoid.
- Se conosci il nemico e te stesso, la tua vittoria è sicura. Se conosci te stesso ma non il nemico, le tue probabilità di vincere e perdere sono uguali. Se non conosci il nemico e nemmeno te stesso, soccomberai in ogni battaglia. (Sun Tzu)
- L'eccessiva confidenza nella propria sicurezza è più pericolosa della consapevole mancanza di sicurezza.

UNIVERSITÀ DEGLI STUDI DI MILANO

Definizione di sicurezza

Non esiste una definizione di "Information Security" universalmente riconosciuta. Possiamo comunque delinearla come **la scienza che studia come proteggere le informazioni elaborate o trasferite elettronicamente da atti indesiderabili che possono avvenire accidentalmente, o essere frutto di azioni colpose o dolose**.

UNIVERSITÀ DEGLI STUDI DI MILANO

Sicurezza

"La sicurezza è studio, sviluppo ed attuazione delle **strategie**, delle **politiche** e dei **piani operativi** volti a **prevenire**, **fronteggiare** e **superare** eventi in prevalenza di natura dolosa e/o colposa, che possono danneggiare le **risorse** materiali, immateriali ed umane di cui l'azienda dispone e necessita per garantirsi un'adeguata capacità concorrenziale nel breve, medio e lungo periodo".

UNI/EN ISO 10459/2015

UNIVERSITÀ DEGLI STUDI DI MILANO

Cybersecurity Act

Il Cybersecurity Act (Regolamento UE 2019/881) definisce la cybersecurity come "l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche" (art. 2, comma 1, n. 1);

UNIVERSITÀ DEGLI STUDI DI MILANO

Minaccia informatica

"minaccia informatica" (art. 2, comma 1, n. 8): "qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone".

UNIVERSITÀ DEGLI STUDI DI MILANO

Sicurezza della rete

Art. 4 comma 2 della Direttiva 1148/2016 (c.d. Direttiva NIS)

"«sicurezza della rete e dei sistemi informativi», la capacità di una rete e dei sistemi informativi di resistere, a un determinato livello di riservatezza, a ogni azione che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati o trasmessi o trattati e dei relativi servizi offerti o accessibili tramite tale rete o sistemi informativi; "

UNIVERSITÀ DEGLI STUDI DI MILANO

Il cosiddetto "parametro RID"

Per valutare la sicurezza di un sistema, di solito, vengono presi in considerazione questi tre elementi:

- **Riservatezza** (i dati devono essere trattati solo dai soggetti autorizzati)
- **Integrità** (i dati non devono subire modifiche non autorizzate)
- **Disponibilità** (i dati devono sempre essere disponibili per i soggetti autorizzati)

UNIVERSITÀ DEGLI STUDI DI MILANO

Resilienza

“Capacità di un sistema di adattarsi alle condizioni d'uso e di resistere all'usura in modo da garantire la disponibilità dei servizi erogati”

UNIVERSITÀ DEGLI STUDI DI MILANO

La sicurezza nel trattamento dei dati personali

Il tema della sicurezza nel trattamento dei dati personali ha conosciuto diversi momenti evolutivi, prima affiancando il testo di legge (D.P.R. 318/99), poi finendo incorporato nel testo di legge (artt. 31-36 e Allegato B del D.Lgs. 196/03) per poi diventare elemento che permea tutto il testo di legge, ispirando nel GDPR l'azione del titolare e del responsabile del trattamento.

UNIVERSITÀ DEGLI STUDI DI MILANO

Cambio di prospettiva

Questo cambio di prospettiva è evidente anche nelle modalità con le quali sono evolute le prescrizioni in materia di sicurezza informatica: da set di istruzioni da dover adottare, alle volte anche in maniera inefficiente, a vere e proprie politiche che il titolare e il responsabile del trattamento devono porre in essere sulla base dell'analisi specifica della loro struttura e delle caratteristiche del trattamento.

UNIVERSITÀ DEGLI STUDI DI MILANO

Risk based approach

- La rappresentazione del trattamento dei dati personali in un'ottica di rischio è diretta derivazione di questa concezione.

- È l'approccio tipico delle normative in materia di compliance.

- Rientra nella cosiddetta preparedness.

UNIVERSITÀ DEGLI STUDI DI MILANO

Centralità del rischio nel GDPR

Dalla Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali:

"Fondamentali fra tali attività [quelle volte a dimostrare l'accountability del titolare n.d.r.] sono quelle connesse al secondo criterio individuato nel regolamento rispetto alla gestione degli obblighi dei titolari, ossia il rischio inerente al trattamento. Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati (si vedano considerando 75-77); tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (si vedano artt. 35-36) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi."

UNIVERSITÀ DEGLI STUDI DI MILANO

Art. 32 comma 1

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del **rischio** di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al **rischio**, che comprendono, tra le altre, se del caso: […]

UNIVERSITÀ DEGLI STUDI DI MILANO

La gestione del rischio digitale

Essa consiste in un insieme di azioni coordinate prese all'interno di un'organizzazione o tra organizzazioni per affrontare i rischi digitali massimizzandone le opportunità;

Si basa su un insieme olistico, sistematico e flessibile di processi ciclici che sono trasparenti e dichiarati;

Questo insieme di processi aiuta ad assicurare che le misure di sicurezza siano appropriate e commisurate con il rischio e con gli obiettivi d'interesse pubblico e privato.

UNIVERSITÀ DEGLI STUDI DI MILANO

La visione olistica della sicurezza

Olismo: la sommatoria funzionale delle parti è sempre maggiore della somma delle prestazioni delle parti prese singolarmente;

La gestione dei rischi in materia di sicurezza informatica deve essere integrata nel pensiero manageriale;

Bisogna abbracciare una visione olistica dei rischi associati ai sistemi di informazione e valutare le minacce conseguenti a eventi materiali, carenze umane, nonché a vulnerabilità tecnologiche e ad aggressioni deliberate;

È fondamentale il dialogo tra tutti gli attori (management, utenti, fornitori) per sviluppare una cultura della sicurezza informatica.

UNIVERSITÀ DEGLI STUDI DI MILANO

Cambio di prospettiva

Nella sua Raccomandazione del 2015 “Digital Security Risk Management for Economic and Social Prosperity”, l’OECD sposta totalmente l’attenzione dai Principi del 2002 sulla sicurezza informatica, dove per “sicurezza” si intendeva la sicurezza dei sistemi e delle reti di comunicazione, a una visione di “sicurezza” come protezione delle attività pubbliche e private dipendenti da un ambiente digitale.

UNIVERSITÀ DEGLI STUDI DI MILANO

Definizione di "rischio digitale" per l'OECD

- Il rischio digitale è quella categoria di rischio correlata all'uso, sviluppo e gestione dell'ambiente digitale in qualsiasi attività;
- Questo rischio può derivare dalla combinazione di minacce e di vulnerabilità dell'ambiente digitale;
- Può minare il raggiungimento di obiettivi d'interesse pubblico o privato interrompendo la confidenzialità, integrità e disponibilità delle attività o dell'ambiente digitale nella sua interezza;
- È un rischio dinamico per sua stessa natura, che coinvolge il contesto sia fisico sia virtuale, le persone coinvolte nelle attività e i processi organizzativi che supportano queste ultime.

UNIVERSITÀ DEGLI STUDI DI MILANO

I soggetti interessati: gli stakeholders

"Per stakeholder bisogna intendere i governi, le organizzazioni pubbliche e private, e gli individui che fanno affidamento sull'ambiente digitale per tutta o parte delle loro attività economiche e sociali".

UNIVERSITÀ DEGLI STUDI DI MILANO

I principi generali

- Tutti gli stakeholders devono comprendere i rischi della sicurezza digitale e come gestirli;
- Tutti gli stakeholder devono assumersi la responsabilità della gestione del rischio digitale;
- Tutti gli stakeholders devono gestire la sicurezza digitale in maniera trasparente e conforme ai diritti umani e ai valori fondamentali;
- Tutti gli stakeholders devono cooperare tra di loro, anche se appartenenti a diversi Paesi.

UNIVERSITÀ DEGLI STUDI DI MILANO

I principi operativi

- Le figure apicali devono assicurarsi che il rischio digitale sia gestito sulla base di continui risk assessment;
- Le figure apicali devono assicurarsi che le misure di sicurezza siano appropriate e commisurate al rischio;
- Le figure apicali devono considerare il progresso tecnologico;
- Le figure apicali devono strutturare un piano di pronto intervento e di garanzia della continuità operativa.

UNIVERSITÀ DEGLI STUDI DI MILANO

Un approccio completo

L'OECD denuncia come il contenimento del rischio digitale sia stato finora affrontato solo da un punto di vista tecnico, isolandolo dalla generale governance aziendale;

Si suggerisce, invece, di seguire un approccio più completo declinato in:

- Tecnico
- Legale
- Sicurezza nazionale
- Prosperità del settore pubblico e privato

UNIVERSITÀ DEGLI STUDI DI MILANO

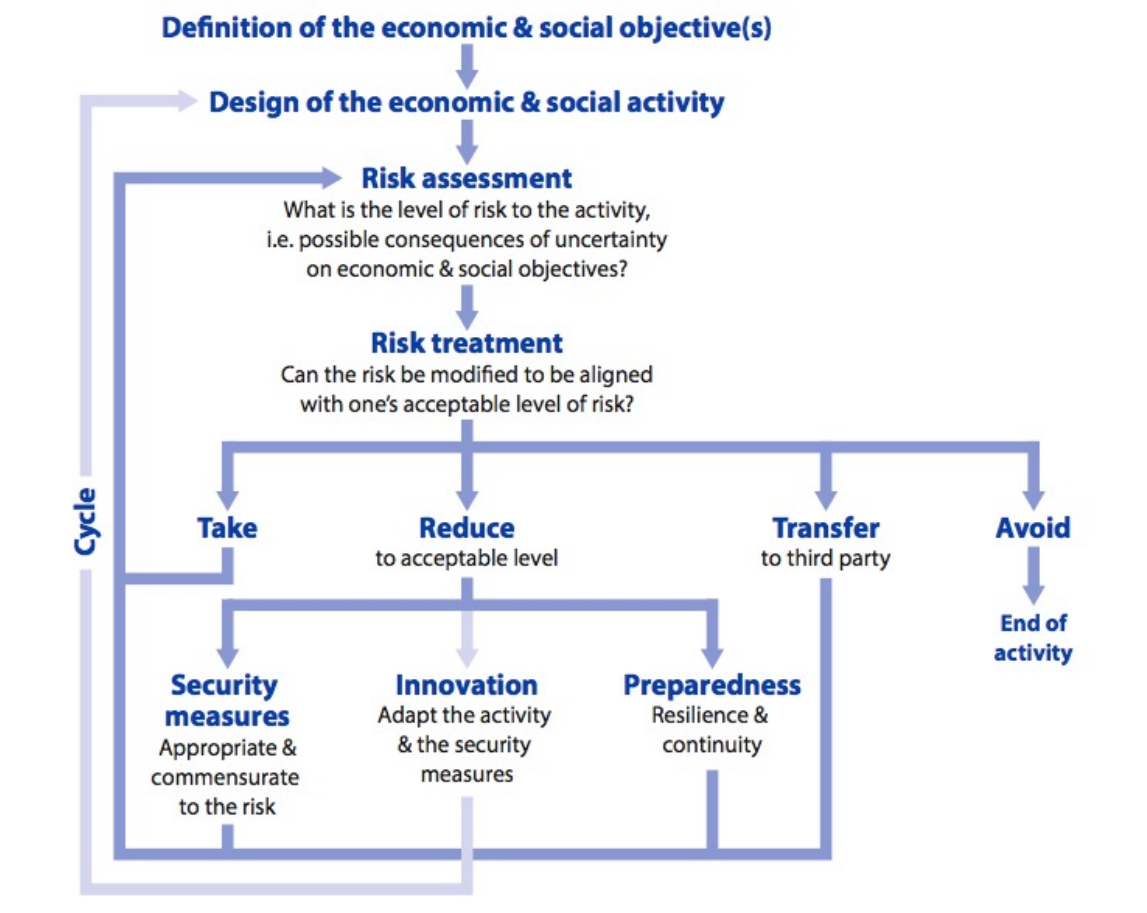
Incidente

Per trovare una definizione bisogna far riferimento all'art. 4 comma 7 della Direttiva NIS

L'incidente è "ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi;"

UNIVERSITÀ DEGLI STUDI DI MILANO

Il ciclo di gestione del rischio digitale secondo l'OCSE



UNIVERSITÀ DEGLI STUDI DI MILANO

Rischio e gestione del rischio nella *data protection*

"Un "rischio" è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. La "gestione dei rischi", invece, può essere definita come l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi"

Art. 29 WP Parere 248 rev 01

UNIVERSITÀ DEGLI STUDI DI MILANO

L’approccio da seguire

Definizione della natura dei dati e degli obiettivi del trattamento

Analisi dei rischi

Progettazione delle contromisure “adeguate”

Redazione di *policies* e verifica delle stesse

UNIVERSITÀ DEGLI STUDI DI MILANO

Le prescrizioni del Garante in merito al rischio

Il Garante, riprendendo una definizione dell'Art. 29 WP, identifica il rischio come "uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità per i diritti e le libertà"

UNIVERSITÀ DEGLI STUDI DI MILANO

Elementi da considerare nell'individuazione del rischio

- Origine
- Natura
- Gravità
- Probabilità
- Impatto sui diritti e le libertà degli interessati

UNIVERSITÀ DEGLI STUDI DI MILANO

Errori da evitare secondo il Garante

La gestione dei rischi non va confusa con il tema delle misure di sicurezza

Il rischio non si riferisce al titolare ma al soggetto interessato

UNIVERSITÀ DEGLI STUDI DI MILANO

Spiegazione

La valutazione del rischio deve riguardare non solo la sicurezza del trattamento ma anche gli effetti complessivi del trattamento.

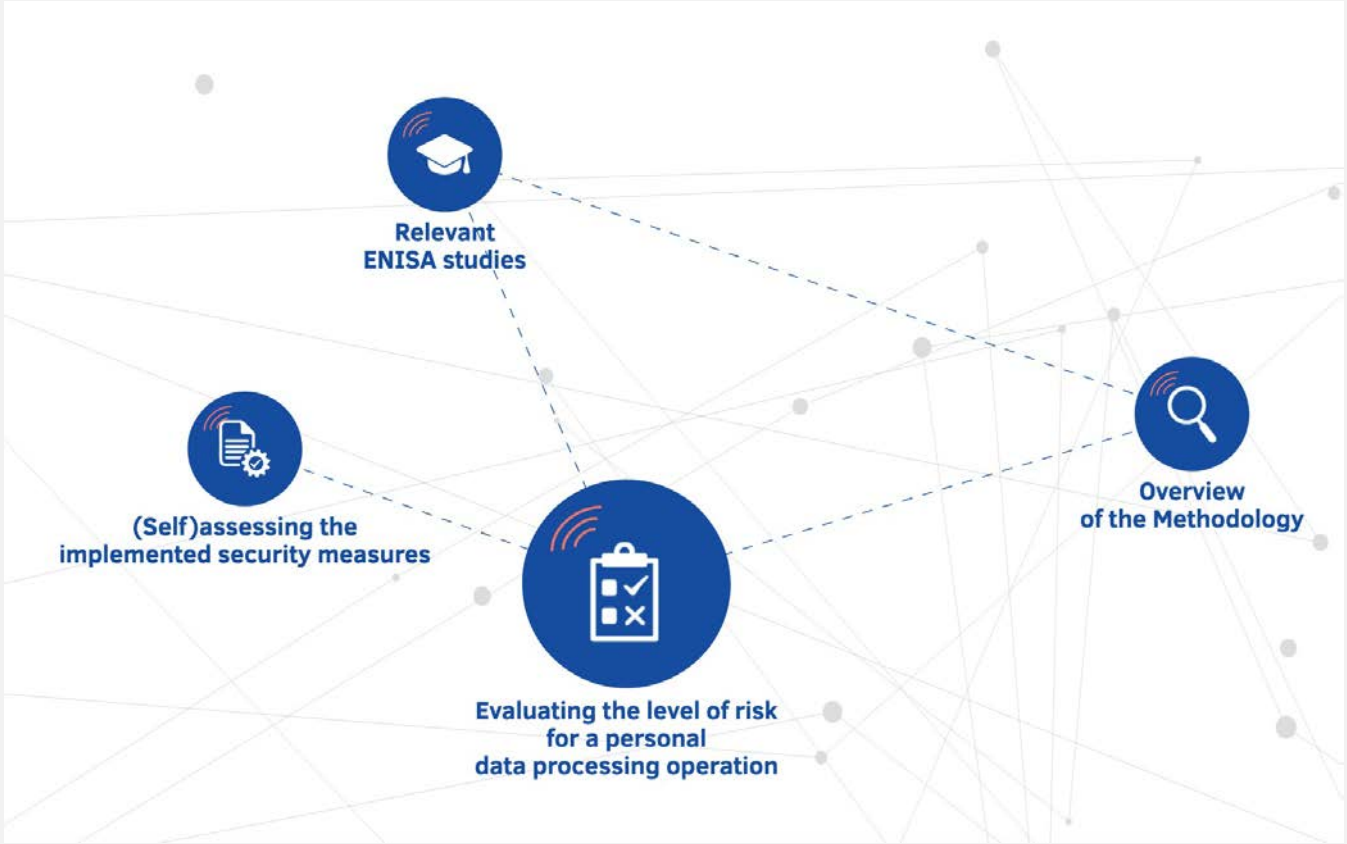
UNIVERSITÀ DEGLI STUDI DI MILANO

Misure per la gestione del rischio

- Misure organizzative (ruoli, governance, istruzioni, formazione, procedure, audit, strumenti di controllo per gli interessati, contatti)
- Misure tecnologiche (policy di sicurezza logiche e fisiche, aggiornamenti ai servizi e ai software, test, controllo accessi e tracciamento operazioni)
- Minimizzazione
- Anonimizzazione dei dati
- Conservazione adeguata
- Cifratura
- Qualità dei dati

UNIVERSITÀ DEGLI STUDI DI MILANO

Tool



https://www.enisa.europa.eu/risk-level-tool/

UNIVERSITÀ DEGLI STUDI DI MILANO

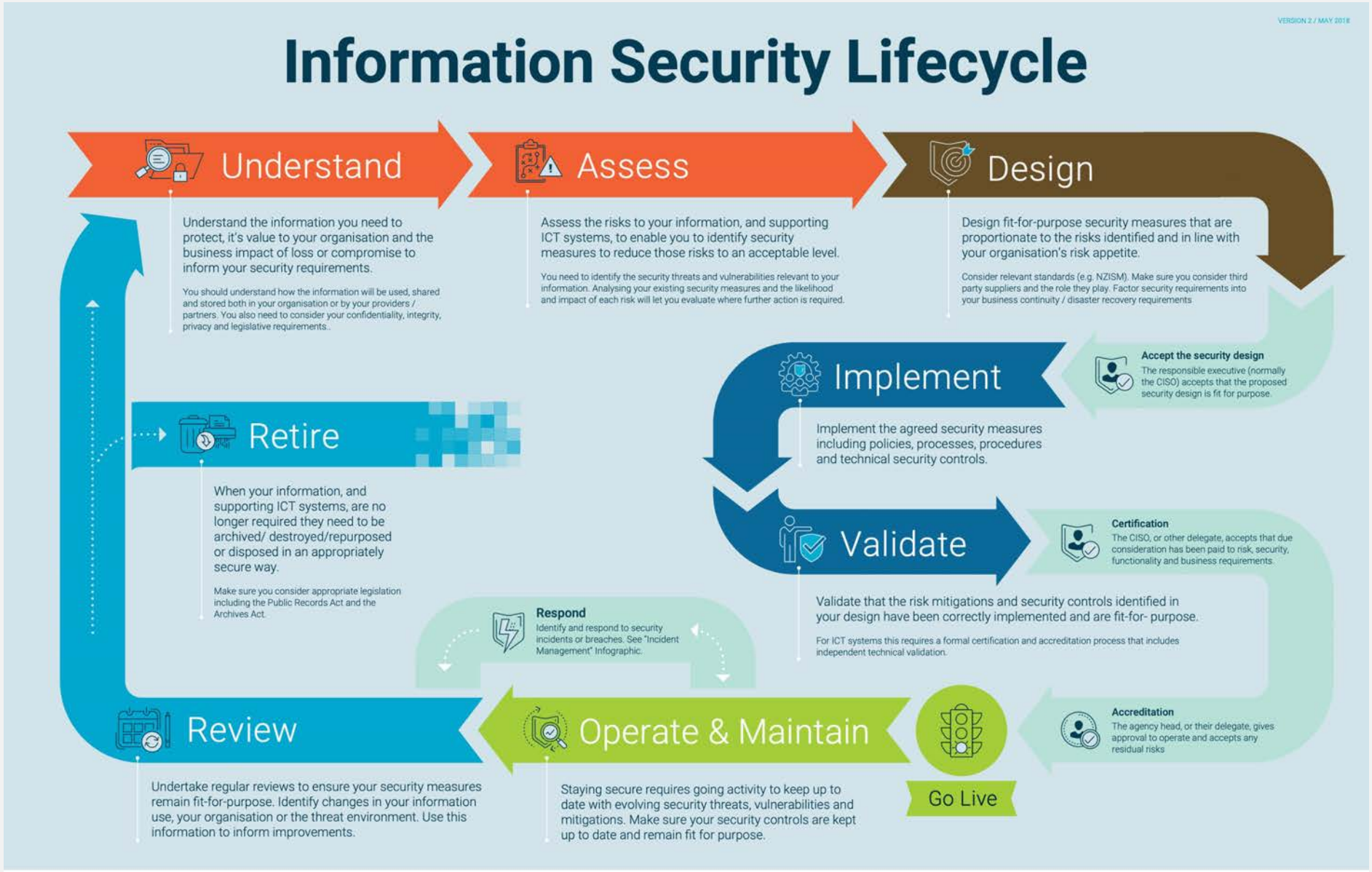
Il "ciclo di Deming" della sicurezza

- Altra caratteristica del GDPR è quello di una concezione "ciclica" della sicurezza.

- Il processo non si esaurisce mai, ma è sempre soggetto a revisioni e aggiustamenti.

UNIVERSITÀ DEGLI STUDI DI MILANO

Information Security Lifecycle



UNIVERSITÀ DEGLI STUDI DI MILANO

Obbligo di sicurezza

- Possiamo quindi dire che il GDPR stabilisce un vero e proprio "obbligo di sicurezza" in capo ai soggetti che trattano dati personali.

- Tale obbligo segue ogni fase del trattamento: dall'origine (Art. 25), alla valutazione (Art. 32, comma 2 e Art. 35), all'implementazione (Art. 32, comma 1), alla gestione dell'incidente (Artt. 33 e 34), fino al risarcimento del danno (Art. 82) e alla sanzione amministrativa (Art. 83, comma 4).

UNIVERSITÀ DEGLI STUDI DI MILANO

Sicurezza e accountability

Art. 24 GDPR commi 1 e 2

“1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, **ed essere in grado di dimostrare**, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l’**attuazione di politiche adeguate** in materia di protezione dei dati da parte del titolare del trattamento."

UNIVERSITÀ DEGLI STUDI DI MILANO

Sicurezza e accountability

Considerando n. 85

"[…] non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, **conformemente al principio di responsabilizzazione**, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche."

UNIVERSITÀ DEGLI STUDI DI MILANO

Sicurezza dei dati

Art. 32 del Regolamento

Tenendo conto dello **stato dell'arte** e dei **costi di attuazione**, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il **titolare** del trattamento e il **responsabile** del trattamento mettono in atto **misure tecniche e organizzative adeguate** per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

- la **pseudonimizzazione** e la **cifratura** dei dati personali;
- la capacità di assicurare su base permanente la **riservatezza**, l'**integrità**, la **disponibilità** e la **resilienza** dei sistemi e dei servizi di trattamento;
- la capacità di **ripristinare tempestivamente** la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- una **procedura** per **testare**, **verificare** e **valutare** regolarmente l'**efficacia** delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

UNIVERSITÀ DEGLI STUDI DI MILANO

Le misure di sicurezza “idonee” nel D.Lgs. 196/03

- Progresso tecnico
- Natura dei dati
- Specifiche caratteristiche del trattamento

UNIVERSITÀ DEGLI STUDI DI MILANO

Le misure tecniche e organizzative "adeguate" nel Regolamento 679/2016

Si fa leva sull'*accountability* dei titolare.

Non più parametri per individuarle ma "suggerimenti" (piuttosto generici) quali:

- pseudonimizzazione e cifratura;
- assicurare su base permanente la riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di trattamento;
- capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative.

UNIVERSITÀ DEGLI STUDI DI MILANO

Politiche di sicurezza

Il GDPR richiede che la sicurezza assolva a tre possibili scenari:

scenario "preventivo", ovvero adottare quelle misure di sicurezza idonee a limitare al massimo il rischio di azioni volte a conoscere illecitamente o a danneggiare i dati personali (es. l'approccio **risk-based** i principi della **minimizzazione** e della **pseudonimizzazione**);

scenario "valutativo", ossia avere le informazioni in merito a natura e distribuzione dei dati all'interno della propria struttura, oltre alle caratteristiche del trattamento, in modo da poter valutare in tempi brevi i rischi connessi a un'eventuale violazione di sicurezza (es. **data protection impact assessment**);

scenario "reattivo" e di contenimento del rischio, ovvero adottare quelle misure di sicurezza che consentano di contenere il rischio di trattamento non autorizzato o non conforme di dati personali e che possano rispondere alla minaccia (es. **notifica della violazione di dati personali**).

UNIVERSITÀ DEGLI STUDI DI MILANO

La policy come componente di una metodologia della sicurezza

Se la definizione di una politica di sicurezza deve tenere conto dei vincoli **tecnici**, **logistici**, **amministrativi**, **politici** ed **economici** imposti dalla struttura ove opera il sistema informativo, è necessario individuare una metodologia di **progettazione**, **realizzazione** e **manutenzione** della sicurezza che, facendo leva su una corretta *policy*, metta in atto un piano per la sicurezza efficace.

UNIVERSITÀ DEGLI STUDI DI MILANO

Fasi di progettazione di una politica di sicurezza

Le fasi principali per una corretta metodologia di progettazione della sicurezza possono essere identificate nelle seguenti:

- ✓ Analisi del contesto;
- ✓ Analisi del sistema informativo;
- ✓ Classificazione degli utenti;
- ✓ Classificazione dei dati trattati;
- ✓ Definizione dei diritti di accesso;
- ✓ Catalogazione degli eventi indesiderati;
- ✓ Valutazione del rischio e della verosimiglianza delle minacce;
- ✓ Individuazione delle contromisure;
- ✓ Integrazione delle contromisure;
- ✓ Verifica della corretta implementazione della politica di sicurezza;
- ✓ Ripetere il ciclo riesaminando tutti gli elementi.

UNIVERSITÀ DEGLI STUDI DI MILANO

Istruire

Art. 32 comma 4 GDPR

"Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri".

UNIVERSITÀ DEGLI STUDI DI MILANO

Formazione e addestramento

Dal Piano nazionale per la protezione cibernetica e la sicurezza informatica

"La formazione e l'addestramento nel settore della sicurezza informatica sono stati, fino ad oggi, orientati prevalentemente al personale specialistico che opera o che è destinato ad operare nel settore. Si pone, pertanto, l'esigenza di un'attività di promozione della cultura della sicurezza informatica diretta ad un ampio pubblico, che includa privati cittadini e personale, sia delle imprese che della Pubblica Amministrazione".

UNIVERSITÀ DEGLI STUDI DI MILANO

Pseudonimizzazione

Art. 4 n. 5)

“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”.

UNIVERSITÀ DEGLI STUDI DI MILANO

Definizione

- Una delle definizioni date in dottrina è la seguente: "la pseudonimizzazione […] consiste nel sostituire un attributo, solitamente univoco, di un dato con un altro, ugualmente univoco e solitamente non intelligibile" cfr. G. D'Acquisto– M. Naldi, Big Data e privacy by design, Giappichelli, 2017, p. 38

- È proprio su quell'univocità che poggia la robustezza del sistema di pseudonimizzazione. Infatti, l'applicazione delle tecniche di pseudonimizzazione su un dato piuttosto che su un altro potrebbe rappresentare l'anello debole del sistema di sicurezza.

UNIVERSITÀ DEGLI STUDI DI MILANO

Esempio

UNIVERSITÀ DEGLI STUDI DI MILANO

La pseudonimizzazione non è la "panacea della sicurezza"

- È evidente che meno saranno i dati sottoposti a pseudonimizzazione o più ridotti saranno i gradi di separazione, più sarà facile superare la misura di sicurezza.
- Uno degli attacchi che viene adoperato nei grandi database, ad esempio, è il c.d. *record linkage attack*, soprattutto quando il database è popolato da molteplici fonti che aumentano determinate ricorrenze (cfr. M. Fiore et al., Privacy of trajectory micro-data : a survey, 2019)

UNIVERSITÀ DEGLI STUDI DI MILANO

Il caso del Governatore del Massachussets

- William Weld, Governatore del Massachussets, subisce una lunga ospedalizzazione che ha grande risonanza pubblica;
- l'assicurazione sanitaria GIC, che annovera tra i suoi clienti anche il Governatore, consegna i dati pseudonimizzati alle autorità competenti ai fini di migliorare la qualità delle cure e controllare la spesa sanitaria;
- uno studente del MIT, Latanya Sweeney, sapendo che il Governatore abitava a Cambridge, acquista per venti dollari l'elenco degli elettori della citta (54.000 abitanti);
- incrociando i dati relativi alle date di nascita, al CAP di residenza e al genere, Sweeney riesce agevolmente a re-identificare il Governatore e a inviargli per posta i suoi dati sanitari (comprensivi di diagnosi e prescrizioni).

UNIVERSITÀ DEGLI STUDI DI MILANO

ENISA e pseudonimizzazione

- Anche l'ENISA si è occupata del tema della pseudonimizzazione, riprendendo alcuni dei concetti affrontati dall'Autorità Garante spagnola.
- In più, tuttavia, l'ENISA illustra i criteri per scegliere un metodo di pseudonimizzazione sulla base del seguente assunto:

UNIVERSITÀ DEGLI STUDI DI MILANO

Pseudonimizzazione vs. anonimizzazione

- La pseudonimizzazione si prefigge un risultato diametralmente opposto rispetto all'anonimizzazione, perché mentre la pseudonimizzazione non modifica l'associazione biunivoca tra dato e persona, con l'adozione di tecniche di anonimizzazione la riferibilità del dato alla persona diventa verosimile quanto un'attribuzione casuale.
- Il dato pseudonimo, quindi, mantiene la natura di dato personale mentre il dato anonimo esce dall'ambito di applicazione del GDPR

UNIVERSITÀ DEGLI STUDI DI MILANO

Si fa presto a dire "cifratura"

Dal Provvedimento del Garante del 4 aprile 2013

- "La predetta comunicazione non è dovuta se il fornitore è in grado di dimostrare al Garante di aver applicato ai dati oggetto della violazione misure tecnologiche di protezione che li hanno resi inintelligibili a chiunque non sia autorizzato ad accedervi […]

- A giudizio dell'Autorità, si considerano inintelligibili i dati che, ad esempio:

  - a. siano stati cifrati in modo sicuro attraverso un **algoritmo standardizzato**, o mediante l'impiego di schemi di cifratura a chiave simmetrica o pubblica noti in letteratura, purché la chiave di decifrazione sia di **adeguata lunghezza** (espressa in numero di bit), sia stata predisposta dal titolare una **policy per la relativa custodia**, e se essa **non sia stata compromessa** da violazioni della sicurezza e sia stata **generata in modo da non consentirne la derivazione** con gli strumenti tecnologici disponibili da parte di soggetti non autorizzati ad accedervi; oppure

  - b. siano stati sostituiti da un valore di hash calcolato attraverso una funzione crittografica di hashing a chiave, purché la chiave utilizzata per effettuare lo hashing dei dati sia di adeguata lunghezza (espressa in numero di bit), sia stata predisposta dal titolare una policy per la relativa custodia, e se essa non sia stata compromessa da violazioni della sicurezza e sia stata generata in modo da non consentirne la derivazione con gli strumenti tecnologici disponibili da parte di soggetti non autorizzati ad accedervi; oppure

  - c. siano stati resi anonimi con procedure tali da non consentire la reidentificazione degli interessati cui si riferiscono da parte di soggetti non legittimati al loro trattamento, anche mediante il ricorso ad altre fonti informative disponibili presso il titolare o pubbliche.

UNIVERSITÀ DEGLI STUDI DI MILANO

Progettare

L’obbligo di assicurare *su base permanente* i requisiti di integrità, riservatezza, disponibilità e resilienza comporta che è diventato indispensabile **progettare** un sistema di sicurezza che tenga conto dei parametri indicati dal legislatore (stato dell’arte, costi di attuazione, natura, oggetto, contesto, finalità del trattamento e rischio per i diritti e le libertà delle persone fisiche)

UNIVERSITÀ DEGLI STUDI DI MILANO

Ripristinare

Diventa indispensabile avere dei piani di *backup* e di *disaster recovery* che possano consentire il **tempestivo** ripristino della disponibilità e accessibilità ai dati

UNIVERSITÀ DEGLI STUDI DI MILANO

Verificare

Il Regolamento sollecita anche l'adozione di procedure di *audit* in quanto utili a testare, verificare e valutare **regolarmente** l'efficacia delle misure tecniche e organizzative adoperate.

UNIVERSITÀ DEGLI STUDI DI MILANO

Lessons learned

I. Utilizzo di HTTPS e di meccanismi di protezione dei dispositivi rimovibili contenenti dati personali (Provv. 17/11/2020)

II. Obbligo di testare l'efficacia delle misure tecniche e organizzative e utilizzo di sistemi di cifratura end-to-end (Provv. 23/01/2020)

III. Obbligo di verifica degli accessi alle applicazioni (Ord. 10/06/2020)

IV. Obbligo di assegnare credenziali di autenticazione univoche (Ord. 26/03/2020)

V. Obbligo di verifica nell'alimentazione e nell'accesso da parte di società partner a un database (Provv. 12/11/2020)

UNIVERSITÀ DEGLI STUDI DI MILANO

Conclusioni

1) La sicurezza è strettamente connessa all'accountability del Titolare

2) La sicurezza è qualcosa che lo stesso Regolamento richiede venga personalizzata sul singolo titolare o responsabile

3) La sicurezza, essendo un obbligo, è connessa alla liceità del trattamento ed è funzionale anche rispetto all'esercizio dei diritti dell'interessato

4) La sicurezza è necessariamente un processo, che deve però essere presidiato

5) La sicurezza richiede continue verifiche e miglioramenti

6) La sicurezza non è un aspetto esclusivamente informatico o tecnico, ma anche organizzativo, logistico, procedurale e normativo.

UNIVERSITÀ DEGLI STUDI DI MILANO

Grazie!

Prof. Avv. Pierluigi Perri

Università degli Studi di Milano

pierluigi.perri@unimi.it

UNIVERSITÀ DEGLI STUDI DI MILANO