STEFANELLI & STEFANELLI STUDIO LEGALE

MSA

Focus sulla Privacy By Design e By Default

Marzo 2022

A cura di Luigi Zampetti

SOMMARIO

1. ORIGINI DELLA PRIVACY BY DESIGN

Negli anni '90, con l'affermarsi del protocollo TCP/IP, della disponibilità delle nuove reti-dati, della nascita delle server farm, della diffusione dei browser che consentivano l'utilizzo di contenuti multimediali abilitando il Word Wide Web, emerse la problematica dell'impatto di queste nuove tecnologie ICT sul diritto degli utenti alla privacy (la "vita privata") e si raccomandò l'utilizzo delle cosiddette ***Privacy Enhancing Technologies*** (PET), tecnologie "aggiuntive", in grado di mitigare i *probabili* effetti lesivi sulla tutela dei dati degli utenti, senza pregiudicare la funzionalità del sistema informativo. [(1)]

Il 24 ottobre 1995 veniva adottata dal Parlamento europeo e dal Consiglio d'Europa la ***Direttiva 95/46/CE*** relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. La Direttiva aveva due obiettivi: il primo, armonizzare le norme adottate nei diversi Paesi (art.1.1), il secondo, non limitare né vietare la libera circolazione dei dati personali (art.1.2), per favorire gli scambi. Nella Direttiva compaiono:

- il termine "confidentiality", che significa "riservatezza" (dei dati) (art.16 Confidentiality of processing)
- l'espressione "at time of the design of" per intendere "al momento della progettazione" (Considerando 46) [(2)].

Nel 2010, la 32ma Conferenza mondiale dei Garanti della privacy [(3)] adottò la ***Resolution on Privacy by design***, secondo la quale la persona è considerata il centro del sistema privacy, e quindi qualsiasi progetto o processo o sistema va realizzato considerando fin dalla progettazione (by design) la riservatezza (confidentiality) e la protezione dei dati personali (data protection). Nella Resolution on Privacy by design venivano anche individuati i sette principi fondamentali che esprimevano pienamente l'intero senso di questa prospettiva.

---

[1] La definizione di riferimento è stata data da Borking and Blarkom et al (1996): "Privacy-Enhancing Technologies è un sistema di misure ICT che protegge la privacy informativa eliminando o riducendo al minimo i dati personali e impedendo così un trattamento non necessario o indesiderato dei dati personale, senza la perdita della funzionalità del sistema informativo."

[2] Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected.

[3] ICDPPC International Conference of Data Protection & Privacy Commissioners - tenutasi a Gerusalemme.

Nella Resolution on Privacy by design furono individuati ***sette principi fondamentali*** che declinano le caratteristiche del sistema di protezione dei dati sin dalla fase di progettazione:

1. ***Proattivo non reattivo*** – prevenire non correggere: agire prima che si sviluppino i problemi.
2. ***Privacy come impostazione di default*** - progettare un sistema IT senza alcuna collezione di informazioni personali e nel caso in cui siano richieste informazioni personali deve sussistere uno scopo o un motivo per raccoglierlo.
3. ***Privacy incorporata nella progettazione*** - la privacy va considerata come fattore per tutta la vita di un progetto.
4. ***Massima funzionalità*** - Valore positivo, non valore zero: su una serie di obiettivi non ne prevale uno solo, ma tutti insieme concorrono alla positiva realizzazione degli obiettivi.
5. ***Sicurezza fino alla fine*** - Piena protezione del ciclo vitale: la sicurezza è il concetto chiave per la privacy, senza di essa non è possibile attribuire nessuna responsabilità e nessun diritto, solo con la sicurezza è possibile assicurare la gestione delle informazioni in maniera corretta per tutto il ciclo di utilizzo delle stesse.
6. ***Visibilità e trasparenza*** - Mantenere la trasparenza: se vengono rispettati gli obiettivi dichiarati, se i documenti utilizzati sono chiari, se le politiche di controllo sono precise sarà possibile instaurare quel grado di fiducia ed affidabilità necessari a permettere ai soggetti interessati di fidarsi.
7. ***Rispetto per la privacy dell'utente*** - Centralità dell'utente: il sistema deve essere pensato e strutturato per gli utenti.

2. PRIVACY BY DESIGN: MISURE E OBIETTIVI

Nel primo decennio degli anni 2000 iniziò a crescere e diffondersi il fenomeno della "digitalizzazione" dei processi e dei servizi, abilitato dalla disponibilità di reti digitali ad alte prestazioni e dalla possibilità di virtualizzare le risorse IT (i due fattori costitutivi del cloud computing), dalla diffusione planetaria delle reti e dei terminali mobili, dei social network, dell'IoT, degli ambienti integrati con i motori di ricerca, dalla costituzione di big data.

L'8 aprile 2016 il Parlamento europeo ed il Consiglio d'Europa adottavano il ***Regolamento 2016/679*** relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (Regolamento Generale sulla Protezione dei Dati). L'articolo 25 del Regolamento ed il Considerando 78, che si ricollegano tanto alla Resolution on Privacy by design quanto al Considerando 46 della Direttiva 95/46/CE, richiedono che siano "messe in atto misure tecniche e organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati, sia al momento di determinare i mezzi del trattamento (by design) sia all'atto del trattamento". Compare inoltre il concetto di "privacy by default" secondo il quale per "impostazione predefinita" sono trattati e protetti solo i dati personali necessari.

Il considerando 78 richiede l'adozione di misure specifiche quali:

1. la minimizzazione dei dati personali trattati [4] e la pseudonimizzazione dei dati personali il più presto possibile [5]
2. la trasparenza per quanto riguarda le funzioni e il trattamento di dati personali
3. il consentire all'interessato di controllare il trattamento dei dati.

Queste misure sono assorbite negli "***obiettivi di protezione specifici per la privacy***" di:

1. **non collegabilità**
2. **trasparenza**
3. **intervenibilità**.

[4] La «minimizzazione dei dati» è richiamata: nell'Articolo 5.1.c "Principi applicabili al trattamento di dati personali"; art. 25.2 "siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento"; Considerando 78 "ridurre al minimo il trattamento dei dati personali".
[5] Art. 25.1; Considerando 78.

Gli obiettivi, i principi di riferimento ed i relativi meccanismi di attuazione sono presenti e/o rintracciabili:

a. nel "***Parere: Privacy e protezione dei dati by design - dalle policy alla progettazione***" dell'Agenzia Europea per la Sicurezza delle reti e dell'informazione (European Union Agency for Network and Information o ***ENISA***) del 2014

b. nelle "***Linee guida per l'adozione di un ciclo di sviluppo di software sicuro***" adottate il 21 novembre 2017 dall'Agenzia per l'Italia Digitale o ***AgID*** (capitolo 10: linee guida per l'implementazione della privacy by design nel SDLC)

c. nella **metodologia *LINDDUN*** di "analisi delle minacce alla privacy nelle architetture software" del 2011 [6]

d. tra i ***principi FIPP*** (Fair Information Practice Principles) del 1974, sui cui si basano quelli della privacy by design [7]

e. nei ***lavori*** di Martin Rost e Andreas Pfitzmann sulla protezione e la sicurezza dei dati del 2009.

Gli obiettivi di trasparenza ed intervenibilità sono anche ricavabili nell'articolo 12 "Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato" inserito nel Sezione 1 - Trasparenza e modalità del CAPO III - Diritti dell'interessato.

Infine, l'obiettivo di trasparenza è presente come principio nr. 10 nella "***Risoluzione di Madrid***" adottata dalla Conferenza internazionale delle autorità di protezione dati e privacy del 5 novembre 2009 sugli "Standard internazionali in materia di protezione dei dati personali e privacy".

[6] Da cui ricavare le contromisure da adottare.

[7] FIPP è l'acronimo generale per un insieme di linee guida che fungono da framework universale per l'integrazione della privacy in tre principali aree di applicazione: 1) tecnologie dell'informazione e della comunicazione, 2) aree di business, 3) progetti fisici e infrastrutturali. Nel corso del tempo molti Paesi ed Organizzazioni hanno declinato le FIP (Fair Information Practices); ad esempio: gli USA come "Privacy and Personal Information Protection" (insieme di indicazioni proposte dalla Federal Trade Commission degli Stati Uniti del 1974), UK come "Data Protection", la UE come "Personal Data Privacy", l'OCSE ha redatto le "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" (linee guida sulla protezione della privacy e sui flussi transfrontalieri di dati personali) basandosi su quelle USA.

3. GLI OBIETTIVI DI PROTEZIONE SPECIFICI PER LA PRIVACY E LE PET

Le misure che consentono di raggiungere i tre obiettivi di protezione specifici per la privacy sono "aggiuntive" alle misure di data protection e costituiscono le Privacy Enhancing Technologies (PET), che, per ENISA, sono una categoria a sé stante **([8])** di tecnologie che riducono al minimo il trattamento dei dati personali e i rischi **([9])**, e facilitano l'adempimento degli obblighi legali di protezione dei dati da parte dei titolari del trattamento dei dati".

In particolare:

1. l'***obiettivo di trasparenza*** (***Transparency***), legato al principio di apertura prerequisito della trasparenza,
   - richiede che tutti i trattamenti di dati rilevanti per la privacy possano essere facilmente compresi e disponibili prima, durante e dopo il trattamento, fornendo informazioni adattate alle capacità del destinatario (interessato).
   - I meccanismi a supporto della trasparenza comprendono la presentazione di tutte le informazioni che riguardano i trattamenti, la comunicazione sia one to many che one to one tra interessati e titolare.
2. l'***obiettivo di intervenibilità*** (Compliance - ***Policy and consent compliance***), legato ai diritti previsti dal Regolamento (artt.15-22),
   - richiede di consentire agli interessati di intervenire su tutti i trattamenti in corso o previsti di dati rilevanti per la loro privacy, anche da parte di coloro i cui dati sono stati cancellati.
   - I meccanismi a supporto dell'intervenibilità comprendono meccanismi, utilizzabili anche in parziale autonomia, per il controllo del trattamento dei dati e richiedere ed ottenere la soddisfazione dei propri diritti (artt.15-22).
3. l'***obiettivo di non-collegabilità*** (***Unlinkability***), legato ai principi di necessità e di minimizzazione dei dati, nonché alla finalità vincolante,
   - richiede che i dati rilevanti per la privacy di una persona fisica (o entità) non possano essere collegabili agli attributi (o descrittori) che ne

[8] Sia nell'ambito dell'informatica, della sicurezza informatica e della crittografia, che del diritto, delle scienze sociali o dell'economia.
[9] Art. 5.1.c del Regolamento.

rappresentano le caratteristiche nello stesso contesto (dataset) o in altri contesti.

- I meccanismi a supporto della non-collegabilità comprendono l'elusione (minimizzazione) dei dati, la pseudonimizzazione, la crittografia, l'anonimizzazione, la separazione dei contesti, la cancellazione dei dati.

Va sottolineato che nel parere ***ENISA*** del 2014 i ***meccanismi a supporto degli obiettivi*** dovrebbero, per quanto possibile:

- essere "***integrati nel trattamento***" senza per questo inficiare la funzionalità del sistema informativo nel quale sono inseriti, specialmente nei sistemi dinamici, cioè nei sistemi che si adattano a requisiti che cambiano,
- e/oppure consistere in "***strumenti utilizzabili anche in parziale autonomia***" dagli interessati,
- ridurre le misure adottate meramente "esterne" al trattamento.

In linea con l'art.25.1 **([10])** ENISA afferma che la Privacy by Design deve essere presa in considerazione durante l'intero ciclo di vita del processo/sistema, dalla progettazione fino al funzionamento del sistema produttivo.

La **variante** "***Data Protection by Design***" del termine "***Privacy by Design***" è stata coniata da ***ENISA*** come "metodo di sviluppo di sistemi e servizi rispettosi della privacy, andando così oltre le semplici soluzioni tecniche e affrontando anche le procedure organizzative e i modelli di business" **([11])**, con l'intento di

- rendere le infrazioni tecnicamente più difficili da attuare,
- contrastare i furti di identità, le frodi e la profilazione discriminatoria,
- effettuare la sorveglianza continua,
- contribuire al rilevamento delle violazioni.

[10] "sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso".
[11] L'estensione dell'ambito della data protection alle procedure organizzative ed ai modelli di business è riscontrabile anche nelle FIPP.

Tabella 1: obiettivi di protezione specifici, meccanismi di supporto e riferimenti al GDPR

OBIETTIVO DI PROTEZIONE SPECIFICO PER LA PRIVACY	**MECCANISMO DI SUPPORTO**	**RIFERIMENTI NEL GDPR** ET AL
Trasparenza	Presentazione di tutte le informazioni che riguardano i trattamenti	Considerando 78, Art. 12 Informazioni, comunicazioni,
	Comunicazione sia one to many che one to one tra interessati e titolare	
Intervenibilità	Controllo del trattamento dei dati da parte dell'interessato, anche in parziale autonomia, e soddisfazione dei propri diritti (artt.15-22)	Considerando 78, Art. 12 modalità trasparenti per l'esercizio dei diritti dell'interessato,
Non collegabilità	Minimizzazione (elusione)	Art. 25.1, 25.2, Considerando 78
	Pseudonimizzazione	Art. 25.1 pseudonimizzazione, Considerando 78 pseudonimizzazione, Art. 32.1.a cifratura
	Crittografia (rendere incomprensibili i dati personali a chiunque senza autorizzazione di accesso)	Art. 32.1.a cifratura, Considerando 83
	Anonimizzazione (trattamento ulteriore che non consenta o non consenta più di identificare l'interessato)	Art. 89.1 "Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici"
	Anonimizzazione (per cancellazione anticipata, effettuata al momento della raccolta)	Parere ENISA - Tecnica di Limitazione dei dati (o mascheramento) (9.3) dello standard BS ISO IEC 20889
	Anonimizzazione (per soppressione / rimozione dei dati)	Parere ENISA - Tecnica di soppressione (o rimozione) (9.3) dello standard BS ISO IEC 20889
	Anonimizzazione (aggregazione dei dati)	Parere ENISA - Tecniche di generalizzazione (9.6) o randomizzazione (9.7) dello standard BS ISO IEC 20889
	Separazione fisica dei dati di contesti diversi	
	Partizione logica dei dati afferenti a processi diversi	
	Cancellazione dei dati	Art. 7, 8, 17

4. MISURE DI DATA PROTECTION NEL GDPR E ISO/IEC 27000

Nel Regolamento, mentre l'art. 25 ed il Considerando 78 tra le misure tecniche e organizzative volte ad attuare i principi di protezione dei dati citano solo la pseudonimizzazione, l'Articolo 32 "Sicurezza del trattamento" affronta specificamente la sicurezza delle informazioni **([12])** richiedendo che la scelta delle misure sia determinata dai rischi presentati dal trattamento **([13])**, e citando ("tra le altre, se del caso") le seguenti misure:

- 32.1a) 34.3a) la cifratura dei dati **([14])**
- 32.1b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento **([15])**
- 32.1c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico **([16])**
- 32.1d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento **([17])**.

4.1 - Misure di data protection nello standard ISO/IEC 27000

La data protection che emerge dagli artt. 25 e 32 rimanda alle misure tecniche e organizzative in grado di difendere e preservare (proteggere) i dati personali rispettando i principi (requisiti) di riservatezza, integrità, disponibilità.

Tali principi sono alla base dello standard ***ISO/IEC 27000*** **([18])** che definisce i requisiti del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) **([19])**, e nell'Annex A contiene i 114 "controlli" (o contromisure) a cui attenersi, suddivisi in 5 macro

[12] Information Security.
[13] Vedi Art. 25.1, Art. 32.1, Considerandi 75, 76, 83.
[14] in ISO/IEC 27000 è richiesto il gruppo di contromisure per la "crittografia".
[15] In ISO/IEC 27000 è richiesto il gruppo di contromisure per la "gestione della Business Continuity".
[16] In ISO/IEC 27000 è richiesto il gruppo di contromisure per la "gestione della Business Continuity".
[17] In ISO/IEC 27000 è richiesto il gruppo di contromisure per "la verifica dell'efficacia delle contromisure adottate".
[18] Lo standard 27000 nel luglio del 2007 ha incorporato lo standard ISO/IEC 17799 "Tecnologia dell'informazione - Codice di condotta per la gestione della sicurezza delle informazioni", il quale, a sua volta, nel 2000 aveva assimilato lo standard BS 7799, pubblicato nel 1995 con le migliori pratiche per la gestione della sicurezza delle informazioni, redatto dal Dipartimento del Commercio e dell'Industria del governo del Regno Unito (DTI), poi arricchito nel 1999 della parte sui "Sistemi di gestione della sicurezza delle informazioni - Specifiche con guida per l'uso".
[19] ISMS: Information Security Management System.

obiettivi: Identificare (ID) Proteggere (PR) Individuare (DE) Rispondere (RS) Recuperare (RC). **([20])**

Le contromisure:

- sono adottate in base ai ***rischi*** che corrono gli asset (ed i dati in essi contenuti) a fronte di vulnerabilità degli asset stessi o ad attacchi interni o esterni;
- includono aspetti relativi alla sicurezza logica, fisica ed organizzativa;
- riguardano tra l'altro
  - il controllo degli accessi logici
  - la crittografia
  - la sicurezza delle comunicazioni e applicativa
  - la relazione con i fornitori coinvolti nella gestione della sicurezza delle informazioni
  - il trattamento degli incidenti (relativi alla sicurezza delle informazioni)
  - la gestione della Business Continuity
  - la verifica dell'efficacia delle contromisure adottate;
- garantiscono nel loro insieme la ***resilienza*** (capacità di reagire ad un impatto senza fermarsi), la ***robustezza*** (efficienza, solidità) e la reattività (capacità di contrastare l'impatto) del sistema informativo.

Lo standard ISO/IEC 27000 si rifà a questi principi manageriali:

- le informazioni sono un asset aziendale,
- le politiche aziendali sulla sicurezza delle informazioni rappresentano un vantaggio competitivo,
- le misure tecniche devono essere proporzionate al rischio ma essere allo stato dell'arte,
- le misure organizzative devono essere compatibili con i processi di produzione ed erogazione pur migliorandone l'aspetto della sicurezza.

[20] Fonte: https://www.csqa.it/.

Tabella 2: contromisure nello standard ISO/IEC 27000 e riferimenti al GDPR.

GRUPPI DI CONTROMISURE IN ISO/IEC 27000	**RIFERIMENTI NEL GDPR**
Rischio	Art. 25.1, Art. 32.1, Considerando 75, 76, 83
Controllo accessi logici	Art. 25.2 accessibilità, Art. 32.1. b riservatezza, Art. 5.1.f integrità e riservatezza
Crittografia	Art. 32.1.a cifratura, Considerando 83
(pseudonimizzazione tramite cifratura)	Art. 25.1 pseudonimizzazione, Considerando 78 pseudonimizzazione, Art. 32.1.a cifratura
(pseudonimizzazione tramite sostituzione)	Art. 25.1 pseudonimizzazione, Considerando 78 pseudonimizzazione
Sicurezza delle comunicazioni e applicativa	Art. 32.1.b riservatezza, integrità, Art. 5.1.f integrità e riservatezza
Relazione con i fornitori	Art. 28 Responsabile del trattamento
Trattamento degli incidenti	Art. 33 Notifica, Art. 34 Comunicazione di una violazione dei dati personali
Business Continuity	Art. 32.1.c Art. 32.1. b disponibilità
Verifica dell'efficacia delle contromisure adottate	Art. 32.1.d valutazione dell'efficacia
Resilienza	Art. 32.1.b resilienza

Il confronto tra i gruppi di contromisure previsti dallo ISO/IEC 27000 e le misure di sicurezza indicate nel GDPR mette in evidenzia che:

- l'approccio basato sul rischio è comune alla sicurezza delle informazioni e dei dati personali;
- le contromisure dello standard ISO/IEC 27000, ricercando la disponibilità, la confidenzialità e l'integrità degli asset informatici, assicurando la riservatezza, l'integrità e la disponibilità dei dati personali trattati con gli asset stessi;
- la certificazione ISO 27000 del sistema informativo, pur non garantendo da sola la conformità al GDPR, può essere considerata una parte rilevante della compliance alla privacy perché ne mette in pratica molti importanti dettati;
- ***senza sicurezza (ISO/IEC 27000) non c'è privacy, ma la sola sicurezza non garantisce la privacy (GDPR)***.

Nel caso il sistema software riguardi il settore della sanità, il confronto con quelle previste dall'***HIPAA*** (Health Insurance Portability and Accountability Act) evidenzia la sovrapponibilità della quasi totalità delle misure ISO/IEC 27000 e derivate dal GDPR.

5. INDIVIDUAZIONE DEI MECCANISMI E DELLE MISURE DI PRIVACY BY DESIGN E DEFAULT

L'analisi Privacy by Design e by Default di un progetto o di un processo o di un servizio si concretizza nel verificare quali Privacy Enhanced Technologies (PET) e quali misure di Data Protection sono state messe in atto per attuare i principi di protezione dei dati, soddisfare i requisiti del regolamento e garantire i diritti degli interessati.

Per individuare i meccanismi e le misure da mettere in atto è stata svolta l'analisi semantica [21] degli articoli del Regolamento relativi ai Principi (Capo II artt. 5-11) ed ai Diritti dell'interessato (Capo III artt. 12-22).

Inoltre, sono stati essere presi in considerazione i seguenti documenti:

a. le "***Linee guida 4/2019 sull'articolo 25 sulla protezione dei dati by design e by default***" adottate il 13 novembre 2019 dal Comitato europeo per la Protezione dei Dati o ***EDPB*** European Data protection Board;
b. il ***Parere: "Privacy e protezione dei dati by design - dalle policy alla progettazione***" dell'Agenzia Europea per la Sicurezza delle reti e dell'informazione (European Union Agency for Network and Information o ***ENISA***) del 2014;
c. nelle "***Linee guida per l'adozione di un ciclo di sviluppo di software sicuro***" adottate il 21 novembre 2017 dall'Agenzia per l'Italia Digitale o ***AgID*** (capitolo 10: linee guida per l'implementazione della privacy by design nel SDLC)
d. le "***Linee guida per la modellazione delle minacce ed individuazione delle azioni di mitigazione conformi ai principi del secure/privacy by design***" (allegato 4 - capitolo 5 progettazione del software secure/privacy by design) adottate il 21 novembre 2017 dall'Agenzia per l'Italia Digitale o ***AgID***;
e. la ***metodologia LINDDUN*** di "analisi delle minacce alla privacy nelle architetture software" del 2011;
f. i ***principi FIPP*** (Fair Information Practice Principles) sui cui si basano quelli della privacy by design.

I meccanismi e le misure individuate sono tra loro ***aggregabili in base a due criteri***:

[21] È l'approccio seguito dall'EDPB per stilare le linee-guida 2019 sull'art.25 del Regolamento.

1. se orientate al rispetto dei principi del GDPR o alla soddisfazione dei diritti degli interessati,
2. l'obiettivo specifico di protezione della privacy e data protection.

6. LA PRIVACY ENGINEERING

6.1 Definizioni generali

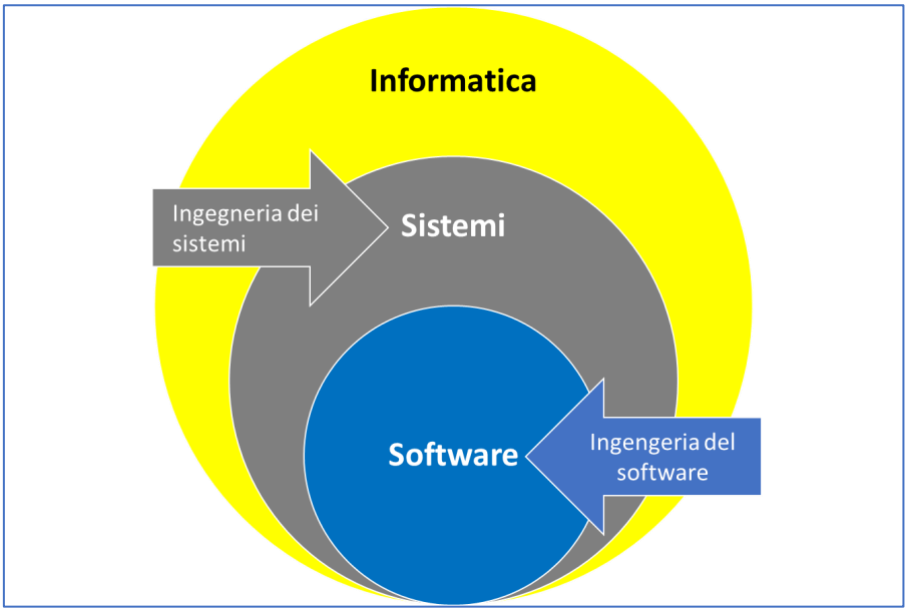
Il software è un "insieme di programmi, procedure, regole, e ogni altra documentazione relativa al funzionamento di un sistema di elaborazione dati" (IEE - Institute of Electrical and Electronic Engineers).

L'ingegneria del software (*Software Engineering*) è un insieme di teorie, metodi e strumenti per sviluppare software di qualità in maniera professionale. In quanto disciplina ingegneristica, fornisce un approccio sistematico e organizzato mettendo a disposizione strumenti e tecniche appropriate al problema da risolvere, ai vincoli di sviluppo, e alle risorse disponibili.

L'obiettivo dell'ingegneria del software è riuscire a sviluppare software in maniera efficace (*functional-effective*) e con costi contenuti (*cost-effective*), in modo che risulti:

- affidabile (dependable o reliable), senza errori
- sicuro (secure), senza vulnerabilità
- usabile (usable), facilmente e logicamente
- efficiente (performing), veloce nell'esecuzione e che richiede poche risorse di elaborazione
- flessibile (configurable) tramite la gestione dei parametri e delle variabili
- modulare (modulate) per essere più controllabile e riusabile
- riusabile (reusable) almeno in parte
- interoperabile (interoperable), capace di interagire con altri sistemi
- manutenibile (maintainable), tempestivamente ed economicamente.

L'informatica si occupa di tutti gli aspetti dello sviluppo del software e dell'evoluzione dei sistemi informatici (processi, architettura, specifiche, applicazioni, database, infrastruttura), comprendendo quindi sia l'ingegneria dei sistemi (***Systems Engineering***) che l'ingegneria del software (***Software Engineering***).



6.2 Metodologie di Software Engineering

I diversi metodi e le diverse tecniche dell'ingegneria del software compongono le metodologie o modelli di processo per gestire i Cicli di Vita del Software (CVS), che:

- definiscono la struttura di massima di software
- indicano le fasi in cui si articola e i criteri di successione del processo di produzione e utilizzo nel tempo.

Sono presenti in letteratura i seguenti **modelli e metodologie**:

- Modello del Prototyping o Sviluppo Evolutivo che produce un prototipo con l'obiettivo di ampliare e chiarire i requisiti e accertare la fattibilità, e dal quale eventualmente partire per aggiungono nuove funzionalità proposte dal cliente.
- Modello sequenziale lineare o a cascata (***Waterfall Model***) che prevede una successione di fasi ben distinte per
    - modellazione dei processi di business,
    - analisi, stesura e convalida dei requisiti,
    - progettazione,
    - sviluppo del codice,
    - test,
    - debug,

    - documentazione,
    - rilascio in esercizio.
- Modello RAD (***Rapid Application Development***) che prevede di suddividere il lavoro in team paralleli (variante del Waterfall).
- Modello COTS (***Commercial-off the-shelf***) ad assemblaggio di componenti preesistenti (anche moduli e sottosistemi) che sono sistematicamente riutilizzati integrandoli con quelli di nuovo sviluppo.
- Modello Incrementale o di Sviluppo iterativo (***Agile Software Development***), nel quale il sistema prodotto e rilasciato non è completo di tutte le funzionalità, ma, ad ogni ciclo, ne sono sviluppate di nuove e/o riviste quelle prodotte, che nell'insieme corrisponderanno al sistema voluto. In genere il rilascio riguarda in successione:
    - le parti dei "servizi" comuni ai moduli/sottosistemi che comporranno alla fine il sistema
    - le parti più critiche (urgenti per il business).
- Modello DevOps (***Development-Operation***s) che risponde all'interdipendenza tra sviluppo software e operations (***variante Agile Software Development***).

6.3 Strumenti di supporto alla Software Engineering

L'applicazione delle metodologie può avvalersi di (*o essere imposta da*) strumenti di supporto delle varie fasi/attività:

1. pianificazione e controllo dei progetti (*Application Lifecycle Management*)
2. progettazione e sviluppo integrato - tipo Upper CASE (*Computer-Aided Software Engineering*) e IDE (*Integrated Development Environment*)
3. testing e debugging - tipo Lower CASE (Computer-Aided Software Engineering) e IDE (Integrated Development Environment)
4. documentazione del codice
5. controllo qualità del codice
6. esame del codice per trovare le vulnerabilità *OWASP* Top 10 - SAST (*Static Application Security Testing*)
7. esame dell'applicazione in esecuzione per trovare vulnerabilità - DAST (*Dynamic Application Security Test*)

8. esame degli ambienti integrati IDE - IAST (*Interactive Application Security*)
9. esame dell'applicazione in esecuzione e interruzione attacco - RASP (*Run-time Application Security Protection*).

6.4 Tipologie di Testing

Le attività di test sono molte variegate e impiegate in base alla struttura del software; possono consistere in:

- test di ogni singolo componente (*Unit testing*)
- test dei componenti tra loro correlati e dipendenti (*Module testing*)
- test dei moduli che compongono un sotto-sistema e delle interfacce (*Sub-system testing*)
- test dell'intero sistema (*System testing*)
- test effettuato su un campione di dati reali insieme al cliente (*Acceptance testing*)
- test su protocolli network, application data e input location (*Fuzz testing*)
- *stress test* sulla validazione dell'input dei dati.

6.5 Le minacce da cui protegge la Software Engineering

La produzione di software presenta due tipi di ***difficoltà***: **([22])**

- le difficoltà "***accidentali***" sono soprattutto legate alle tecnologie (sistemi operativi, ambienti di sviluppo, linguaggi di programmazione) ed al loro utilizzo da parte dei tecnici, che possono generare:
  1. errori di programmazione
  2. vulnerabilità
  3. difficoltà di utilizzo
  4. complessità di interagire con altri sistemi
  5. sforzo per adattarsi a nuovi parametri e variabili;
- le difficoltà "***essenziali***" sono invece legate a:
  1. la complessità dei problemi che il software deve modellare e controllare (complexity);

[22] Fred Brooks, 1986: "No Silver Bullet - Essence and Accident of Software Engineering".

2. la necessità di conformarsi a regole/ interfacce variabili e non derivate da un modello fisico-matematico (conformity);
3. la mutevolezza nel tempo dei requisiti su cui produrre il software (changeability);
4. la difficoltà di avere (e controllare) la visione d'insieme delle funzionalità-utente e dei meccanismi che le abilitano (invisibility).

6.6 Software & Systems Engineering: modellazione delle minacce e obiettivi

Dall'analisi di framework, metodologie e guide per lo sviluppo sicuro delle applicazioni software emerge che:

- durante la fase di progettazione l'attività di modellazione delle minacce, ovvero l'individuazione, classificazione e peso dei difetti di sicurezza, delle vulnerabilità che possono concretizzare le minacce alla sicurezza dell'informazione e dei sistemi, è centrale e permette di definire le contromisure e la priorità di adozione;
- durante la fase di sviluppo si possono utilizzare tecniche e tool a supporto della qualità o sanità del codice;
- dopo la fase di sviluppo si utilizzano tecniche e tool per individuare le vulnerabilità ed i bug (testing).

In conclusione, gli obiettivi della Software & Systems Engineering sono:

1. la qualità ambientale (affidabilità degli strumenti e delle tecniche
2. la qualità strutturale (solidità di ingegnerizzazione dell'architettura e sanità del codice).

7. INDIVIDUAZIONE DELLE MISURE PER L'ANALISI PRIVACY ENGINEERING

Secondo il National Institute of Standards and Technology (NIST) la Privacy Engineering "Si concentra sulla fornitura di indicazioni che possono essere utilizzate per ridurre i rischi per la privacy e consentire alle organizzazioni di prendere decisioni mirate sull'allocazione delle risorse e sull'efficace attuazione dei controlli nei sistemi di gestione delle informazioni. "

Su questa linea, l'analisi Privacy Engineering consiste nel verificare quali misure sono state messe in atto per rispettare i requisiti di sicurezza e privacy.

L'***individuazione delle misure*** è stata effettuata prendendo in considerazione:

a. nel "***Parere: Privacy e protezione dei dati by design - dalle policy alla progettazione***" dell'Agenzia Europea per la Sicurezza delle reti e dell'informazione (European Union Agency for Network and Information o ***ENISA***) del 2014;

b. nelle "***Linee guida per l'adozione di un ciclo di sviluppo di software sicuro***" adottate il 21 novembre 2017 dall'Agenzia per l'Italia Digitale o ***AgID*** (capitolo 10: linee guida per l'implementazione della privacy by design nel SDLC);

c. le "***Linee guida per la modellazione delle minacce ed individuazione delle azioni di mitigazione conformi ai principi del secure/privacy by design***" (allegato 4 - capitolo 5 progettazione del software secure/privacy by design) dell'AgID del 21 novembre 2017;

d. le "***Linee guida per lo sviluppo sciuro***" (allegato 2) adottate il 21 novembre 2017 dall'Agenzia per l'Italia Digitale o ***AgID***;

e. le "***Linee guida sulla sicurezza nel procurement ICT***" adottate a luglio 2019 dall'Agenzia per l'Italia Digitale o ***AgID***;

f. nella **metodologia *LINDDUN*** di "analisi delle minacce alla privacy nelle architetture software" del 2011;

g. tra i ***principi FIPP*** (Fair Information Practice Principles) del 1974, sui cui si basano quelli della privacy by design, e dai quali ricavare le misure per rispettarli;

h. le ***proprietà della sicurezza*** (vedi norma ISO 1779914) che sviluppano il principio FIPP di "Integrità/Sicurezza";

i. la ***metodologia*** di Software Analysis e Measurement del ***CAST*** (Center for Applied Special Technology);

j. lo ***standard*** per la protezione delle informazioni sanitarie protette (PHI, Protected Health Information) ***HIPAA*** (Health Insurance Portability and Accountability Act.

Ne emerge che "***la Privacy Engineering è l'insieme di metodi, tecniche e strumenti per implementare la privacy quale attributo di qualità della Software & Systems Engineering***" (definizione dell'AgID).

Da notare che, sia nel parere di ENISA che nei principi FIPP, l'implementazione della "Privacy by Design" (o "Data Protection by Design" secondo ENISA) si estende, oltre

che alle soluzioni tecniche, anche alle procedure organizzative ed ai modelli di business. (vedi il successivo paragrafo 9)

I metodi, le tecniche e gli strumenti individuati sono tra loro aggregabili in base a tre criteri:

1. quelli che riguardano la fase di produzione del software e sono di competenza del provider,
2. quelli che interessano la fase di esercizio-utilizzo e sono di competenza del provider,
3. quelli che interessano la fase di esercizio-utilizzo e sono di competenza dell'operatore.

8. LE CHECK LIST DI AUTOVALUTAZIONE

8.1 Cosa sono le check list

L'analisi dell'eventuale gap tra i meccanismi e le misure individuate nei vari documenti (normative e standard) e quelle messa in atto dall'organizzazione per rispondere ai requisiti di Data Protection by design e Privacy Engineering può essere eseguita in autovalutazione utilizzando le apposite check list ASG679© della Stefanelli & Stefanelli Servizi Legali.

Le check list sono composte da elenchi di domande dedicate ad analizzare la situazione del singolo dispositivo medico, ove possibile sono completate dai riferimenti normativi che ne giustificano la presenza, e dalle raccomandazioni da seguire non sia adeguata.

8.2 La generazione del report ed il risk rate

La compilazione di tutte le domande incluse in una check list determina la generazione automatica del report finale nel quale sono riportate queste informazioni:

1. nome e cognome del compilatore,
2. la specificazione del progetto e del processo o del servizio o del sistema oggetto d'analisi,
3. le domande poste,
4. le risposte date dall'utente,
5. il livello di rischio di violazione dei requisiti di sicurezza (riservatezza, integrità, disponibilità) o risk rate.

Il risk rate è automaticamente calcolato in base alle risposte date dall'utente in quanto, ad ogni risposta, è associato un peso su una scala a quattro valori

1 = Low | 2 = Medium | 3 = High | 0 = Null

Il peso, attribuito dall'auditor nella fase di realizzazione del sistema, è trasparente per il compilatore per non influenzare la scelta della risposta.

Il risk rate è rappresentato graficamente con i colori:

 Rosso = rischio alto  Giallo = rischio medio  Verde = rischio basso.

9. SUI PROCESSI AZIENDALI

Con il termine "processo" si intende la "successione di attività tra loro collegate logicamente e finalizzate a raggiungere un risultato, svolte con determinate modalità e impiegando specifici mezzi".

Ogni processo si caratterizza per:

1. l'utilizzo di input, e cioè di risorse in entrata o di partenza,
2. l'interazione con altri processi svolti all'interno o all'esterno dell'organizzazione, e
3. la produzione di output come risultato delle attività di quel processo.

Sono distinguibili due tipi di processo:

1. i processi "primari" o "core" sono quelli il cui output genera valore per gli stakeholders (azionisti, manager, dipendenti, fornitori, utenti, istituzioni, ambiente, ecc),
2. i processi "di supporto" sono quelli che forniscono input e informazioni "di servizio" necessari ai processi primari.

Le risorse coinvolte nello svolgimento dei processi sono di otto tipologie:

1. risorse umane (Personale interno ed esterno),
2. risorse organizzativo e procedurale
3. risorse tecniche
4. know-how (brevetti e partnership),
5. reputazionale,
6. logistico (uffici, magazzini, fabbriche),
7. economico-finanziario,
8. informativo (dati, informazioni).

Va sottolineato che, quando un processo soggetto a valutazione del rischio evidenzia un forte criticità, l'organizzazione è chiamata ad effettuare:

- interventi di tipo incrementale, volti cioè al continuo e graduale miglioramento dei processi, noti anche col termine di Business Process Improvement (BPI),

oppure

- interventi di tipo radicale e cioè volti al completo ridisegno del processo, noti col termine di Business Process Reengineering (BPR).

10. IL CONCETTO DI "RISCHIO"

In ambito security e privacy, il rischio è valutato stimando gli effetti (il danno o impatto) di un evento negativo (il concretizzarsi di una minaccia) in base alla probabilità che accada.

Il rischio è quindi un concetto probabilistico e sono possibili tre diversi **metodi di** (analisi e) **valutazione**:

1. qualitativo che richiede di esprimere un giudizio sulla situazione che si sta valutando su una scala qualitativa (ad esempio alto, medio, basso; oppure improbabile, poco probabile, probabile, altamente probabile);
2. quantitativo nel quale la valutazione è espressa in valori numerici riferiti al valore economico sia dei singoli asset che costituiscono il perimetro di analisi che degli specifici danni (perdite) prodotti dal concretizzarsi dei rischi;
3. semi quantitativo nel quale la valutazione è effettuata in termini qualitativi e poi trasformata in valori numerici (pesi) per poterla sottoporre ad algoritmi di calcolo, come se fosse una valutazione quantitativa.

10.1 - L'attribuzione dei pesi

Questa operazione, che è discriminante per trasformare un metodo di valutazione qualitativo in semi quantitativo, è compiuta dall'auditor in base a:

- la riferibilità a best practices applicabili al singolo elemento,
- la specificità del contesto in cui è collocato/agisce l'elemento,
- le competenze acquisite nel tempo,
- l'esperienza lavorativa e professionale.

10.2 - La soluzione ASG679©

Al termine dell'attività di compilazione delle check list dedicate la valutazione del rischio risulterà di tipo semi quantitativo.

10.3 - Le check list specifiche

Nella tabella sono elencate le 9 check list tra loro complementari per eseguire in autonomia la valutazione del rispetto delle misure e dei meccanismi individuati relativi a:

- ad un processo aziendale, ad un progetto da realizzare o un servizio da erogare (check list L1, L2, L3, L4),
- alla soluzione software utilizzata a supporto del processo / progetto / servizio (check list M1, M2, M3)
- ad un applicativo software prodotto da una software house e adoperato da terzi (check list M1, M2, M3, M4, M5).

Obiettivo dell'analisi	Nr	Check list da utilizzare	Ambiti e perimetri dell'analisi	
Privacy by design / default	**L3**	Rispettare i principi (artt. 5-11 del GDPR) raggiungendo l'obiettivo di protezione specifico della privacy della "trasparenza".	**Processo / Progetto / Servizio**	
	L4	Soddisfare i diritti (artt. 12-22 del GDPR) raggiungendo l'obiettivo di protezione specifico della privacy della "trasparenza".		
	L1	Rispettare i principi (artt. 5-11 del GDPR) raggiungendo l'obiettivo di protezione specifico della privacy di "intervenibilità".		
	L2	Soddisfare i diritti (artt. 12-22 del GDPR) raggiungendo l'obiettivo di protezione specifico della privacy di "intervenibilità".		
	M2	Rispettare i principi (artt. 5-11 del GDPR) e raggiungere l'obiettivo di protezione specifico della privacy di "non collegabilità".	**Software di supporto al processo / progetto / servizio**	**Applicativo software utilizzato da terzi**