Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea in Informatica

Privacy By Design e Data Protection Officer: aspetti normativi e buone prassi nel trattamento dei dati personali.

Relatore:
Chiar.ma Prof.sa
Raffaella Brighi

Co-Relatore:
Chiar.ma Dot.sa
Daniela Prestipino

Presentata da:
Elena Fabbri

Sessione III
Anno Accademico 2013-2014

A Stefano,
mia ancora nell'immenso mare della vita.
A Stefania,
la mia mamma, la mia roccia, la mia forza.
A Mirca, Lisa, Raffaele, Laura,
Lorenzo, Alberto, Valentina, Filippo,
i migliori amici che si possano incontrare ...

Introduzione

La rivoluzione tecnologica avvenuta nell'ultimo secolo ha toccato vari aspetti, compreso quello della comunicazione. Il primo esempio in questo campo è stata la tecnologia EDI (Electronic Data Interchange), che permetteva un interscambio di informazioni fra due sistemi informativi utilizzando un canale dedicato, limitando al minimo l'intervento umano.

L'avvento di Internet con il WWW e le sue evoluzioni sino all'affermazione dei Social Media hanno modificato radicalmente il metodo di comunicazione, ampliando notevolmente il numero di dispositivi comunicanti. L'arrivo delle reti mobili ha permesso l'ampliamento degli oggetti comunicanti, comprendendo smartphone e tablet.

L'ultima rivoluzione in questo campo è dettata da Internet of Things, termine indicante un'ulteriore estensione della comunicazione, non più legata solo alle persone, bensì agli oggetti, sensorizzati ed eterogenei, che interconnessi raccolgono e collezionano flussi di dati la cui elaborazione e gestione favorisce una rappresentazione digitale e smart (intelligente) del mondo reale. IoT ha drasticamente aumentato la pervasività della rete e gli oggetti (devices) tendono ad acquisire identità digitale al pari degli utenti nella misura in cui sono abilitati ad accedere a servizi ed informazioni.

I vantaggi sono intuibili e tutti sostanzialmente legati ad un più ottimale e efficace gestione delle risorse orientate al miglioramento della qualità della vita degli utenti e alla possibilità di fornire loro servizi altamente personalizzati. Ad esempio per le c.d. Smart Cities (gestione del traffico, dell'ambiente e della gestione dei rifiuti); per la gestione delle reti di servizi e relativo monitoraggio degli impianti sia a fini manutentivi che si sicurezza; per il controllo e la tracciabilità delle filiere di produzione; o anche per l'ambito sanitario

per le applicazioni di telemedicina.

Ma sono altrettanto intuibili gli svantaggi tutti sostanzialmente legati alla preoccupazione che questi oggetti resi intelligenti perché interconnessi acquisiscano informazioni personali, violandone la riservatezza e divulgandole fuori controllo dell'utente proprietario a soggetti non autorizzati. Le immediate conseguenze: impersonazione, furto di informazioni e di identità, violazione dell'anonimato convergono tutte verso una perdita di fiducia dell'utente verso le reti e i servizi digitali.

Per questo è importante costruire strumenti tali per cui non sia possibile, ad agenti esterni, prelevare dati per compiere azioni di varia natura. I progettisti non hanno solo il compito di definire sistemi funzionanti, bensì hanno come compito principale quello di definire sistemi sicuri per gli utilizzatori degli stessi.

Ma cosa vuol dire sicuro?

Il concetto è ampio e ricco di letteratura a supporto: spesso con sicuro si intende nascosto, celato, riservato. Ma non è necessariamente così; se i dati fossero celati, riservati, i progettisti non potrebbero utilizzarli nei sistemi, rendendo quindi gli stessi inutilizzabili. Per questo, ad oggi, il termine riservato è, tra l'altro, correlato ad accedibile e valido; presupposti tali che le informazioni risulteranno confidenziali agli esterni, controllabili dai soggetti interessati, ma utilizzabili dagli sviluppatori (ovvero da chi ne implementa trattamento e processamento) per le relative esigenze.

Il legislatore Italiano ed Europeo lavorano da anni per definire, al meglio, il concetto di sicurezza legato ai dati, definendo questa materia come **Protezione dei Dati Personali**. La stessa così definisce il dato personale:

> ..., qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;[1]

Questa materia è in continua evoluzione, dato il progresso tecnologico in atto; quello che si sta studiando da anni è la definizione di un impianto di

[1] art. 4, comma 1, capo b, D.Lgs 30 giugno 2003, n.196 *Codice in materia di protezione dei dati personali.*

base che sia valido per il lungo periodo, integrato con parti aggiornate molto frequentemente per garantire la validità del testo stesso.

Date queste premesse, il filo conduttore della seguente Tesi sarà le modalità di utilizzazione degli strumenti digitali per il trattamento dei dati personali, in relazione ai vincoli normativi, alle criticità e ai rischi, nonché alle contromisure consolidate ed emergenti legate al processamento.

L'analisi sarà mirata a creare un semplice strumento di supporto per chi affronta per la prima volta questi problemi, tenendo conto che l'implementazione di un sistema di dati personali necessita non solo di conoscenze tecniche e tecnologiche, ma anche di conoscenze giuridiche e gestionali.

Il percorso scelto terrà conto dell'evoluzione nel tempo del quadro normativo e tecnologico connesso alla protezione dei dati personali. Per quando attiene il quadro normativo è giunto alla fase conclusiva, e se attende approvazione e ratifica, il percorso legislativo del Regolamento Europeo 2012/0011 riguardante il trattamento dei dati personali e la libera circolazion degli stessi. Questo testo - regolamento generale sulla protezione dei dati personali, redatto dal Parlamento Europeo e dal Consiglio dell'Unione Europea - affiancato da efficaci e fattive misure di attuazione, ed indicando qui principi cardine necessari a definire un testo di lunga durata, pone ad obiettivo l'armonizzazione della materia in tutto il territorio comunitario; lo sviluppo dell'economia digitale nel mercato interno minimizzando la percezione che le operazioni on-line comportino notevoli rischi; il controllo dei soggetti interessati dei propri dati personali; certezza giuridica ed operativa per i soggetti economici e le autorità pubbliche. La stessa proposta di regolamento, oltre a contenere una serie di regole di progrettazione ad obbligatoria applicazione introduce nuovi attori e nuove figure professionali.

Per quanto attiene il quadro tecnologico saranno illustrate le metodologie consolidate rientranti nelle Privacy Enhanced Technologies (PETs) e l'approccio emergente, complementare a queste ultime, del Privacy By Design (PbD). Le PETs rappresentano un insieme di tecnologie integrate in servizi ed applicazioni, di per se insicure - perchè progettate tali, senza includere specifiche di protezione delle informazioni - con le finalità di proteggere la gestione e lo scambio di dati personali. Il PbD rappresenta un insieme di principi, prassi (prima) e tecnologie (dopo) con le quali sin dalla fase di piani-

ficazione si progetta un sistema con intrinseche caratteristiche di sicurezza. La protezione dei dati personali diventa quindi una specifica predefinita e non integrabile a posteriori in risposta all'esito di specifiche criticità.

Esposte queste premesse la testi sarà così strutturata: la prima parte descrive il concetto di privacy e le relative minacce e contromisure (tradizionali ed emergenti) con riferimento ai contesti di gestione (aziendale e Big Data) e al quadro normativo vigente. La seconda parteillustra in dettaglio i principi e le prassi del *Privacy by Design* e la figura del *Privacy Officer* formalmente riconosciuta dal novellato giuridico. La terza parte illustra il caso di studio nel quale vengono analizzate tramite una tabella comparativa minacce e contromisure rilevabili in un contesto aziendale. A chiusura sono esposte le conclusioni e i riferimenti bibliografici.

Indice

Parte I

Stato dell'Arte

Capitolo 1

Privacy e Protezione dei Dati Personali

Con il termine *privacy* si intende il diritto alla riservatezza della propria vita privata, e di conseguenza, alle informazioni riguardanti essa stessa. La tutela di queste ultime è fondamentale in primo luogo per la natura delle stesse: il termine privacy non attiene solamente informazioni atte al riconoscimento, bensì dati legati a salute, preferenze sessuali, e così via. Si comprende quindi l'importanza della tutela al diritto alla privacy alla protezione dei dati personali - diritti fondamentali - così come stabilito nella Costituzione Italiana e nella Carta dei Diritti Fondamentali della Unione Europea.

Altro punto di analisi riugarda la serie di comportamenti illeciti legati all'appropriazione indebita e all'utilizzo dei dati. Il mercato nero legato alle informazioni personali è in rapida crescita. Fonti WEF (Word Economic Forum) stimano sino a tremina miliardi di dollari nei prossimi sei anni le perdite legate alla gestione illecita di identità ed informazioni, e dati McAfee stimano il costo gobale del cyber crime tra i trecentosettantacinque e i cinquecentosettantacinque miliardi di dollari [1]

Oggetto di analisi di questo capitolo è la definizione di privacy e dato personale, analizzando due ambiti specifici; il contesto aziendale e quello più ampio di internet.

1.1 Social Network e Big Data

Un servizio di social network (rete sociale) consiste nella creazione e nel controllo di reti sociali online destinate a comunità di soggetti che condividono determinati interessi e attività, ovvero intendono esplorare gli interessi e le attività di altri soggetti, attraverso l'impiego di applicazioni software. Si tratta in maggioranza di servizi basati sull'utilizzo del web; numerose sono le modalità di interazione fra gli utenti [...] [2].

L'avvento e la crescita di questi servizi ha cambiato radicalmente la modalità di accesso alla vita pubblica. Grandi quantità di dati, non solo di tipo identificativo, vengono raggruppato insieme per formare insiemi particolarmente numerati ed eterogenei in quanto popolati da dati provenienti da fonti dati diverse. Questi oggetti assumono il nome di **Big Data**, e godono di una serie di caratteristiche [3]:

- volume: la quantità, e quindi, la numerosità dei dati;
- varietà: l'eterogeneità dei dati contenuti;
- velocità: la celerità di produzione ed elaborazione delle informazioni.

Per spiegare l'importanza dei Big Data, soprattutto se contenenti Dati Personali, si utilizzeranno le parole di Research Scientist J. H. Clippinger:

> In un certo senso i dati personali sono la tipologia di Big Data più importante perché sono i dati più sensibili, predittivi, privati e preziosi. I Big Data non sono solo una questione di quantità dei dati processati, ma anche di qualità, valore e privatezza di quei dati. Tutti, aziende, imprese e quant'altro, vogliono che i dati personali rientrino nelle loro analytics dei Big Data [4].

Si deduce l'importanza della gestione di codesti dati, ed in particolare si sottolineano due nuove dimensioni che ne motivano la protezione, oltre al mantenimento della riservatezza: valore e qualità. Una quarta V affiancata alle tre canoniche dei Big Data è quella riferita alla veridicità, ovvero attinenza e coerenza dei contenuti.

1.2 Contesti Organizzativi Aziendali

In contesto aziendale, il trattamento dei dati personali è richiesto per adempiere ad una serie di obblighi aziendali, non solo verso il dipendende per il rispetto del contratto individuale stipulato, ma anche verso lo Stato, nel rispetto degli obblighi amministrativi. Esempi in questo ambito possono riguardare i dati necessari al calcolo di compensi o premi, oppure calcoli pensionistici o previdenziali, oppure, infine fruizione di permessi sindacali o stipendi [5].

L'impiego di tecnologie digitali, connessioni ad internet, utilizzo di posta elettronica, costituiscono oggi strumenti indispensabili strumenti di lavoro, capaci di rendere l'esecuzione della prestazione lavorativa più efficiente e più rapida. Se da una parte l'innovazione tecnologica comporta una rivoluzione nei metodi di lavoro e nelle forme organizzative, dall'altra permette di raccogliere con maggiore facilità rispetto al passato dati personali attinenti al dipendente, oltre all'accesso ad informazioni prima non facilmente possibile [6].

Le nuove tecnologie informatiche permettono, ad oggi, di raccogliere, manipolare, trattare dati in maniera tale da minare il diritto alla riservatezza dei dipendenti. Le possibilità in capo al datore di lavoro di controllare i propri sottoposti, in maniera diretta od indiretta, sono aumentate e il rischio di essere controllati da parte del datore di lavoro non solo per la propria persona, ma anche per il lavoro svolto con modalità e per fini non legittimi, e in alcuni casi lesivi di interessi tutelati specificamente quali il diritto alla privacy, alla dignità e alla riservatezza del lavoratore.

Non si vuole certo limitare il datore di lavoro, che ha comunque il potere di agire e di fare indagini, purché siano compiute su fatti attinenti e rilevanti rispetto alle valutazioni attitudinali, in diretta connessione alle mansioni affidate. Ma l'analisi di circostanze extra-lavorative non costituisce una causa di licenziamento, se non in casi cui la natura del lavoro e la delicatezza della posizione richiedano il non succedersi di taluni eventi.

La natura fiduciara del rapporto di lavoro unita alla delicatezza di informazioni legate ai dipendenti ha richiesto un impianto normativo più specifico ed adatto; rimanendo saldi i principi cardine indicati nel Codice della Priva-

cy, il Garante per la Protezione dei Dati ha previsto una serie di Linee Guida da applicare in ambito aziendale: *Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datorid di lavoro privati*, *Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporot di lavoro in ambito pubblico*, *Linee guida del Garante per posta elettronica e Internet*.

Un corretto trattamento di dati può essere visto come una risorsa sia dai clienti, che posso apprezzare un punto positivo per costruire una fiducia sul mercato ed apliare così le possibilità di guadagno. D'altro lato, la sicurezza informatica è requisito fondamentale in ambito aziendale soprattutto in materia di trattamento dei dati; i continui e sempre più complessi attacchi informatici effettuati anche con tecniche di tipo phishing, spam o DoS furto d'identità, possono costituire vere e proprie vulnerabilità per l'azienda. E' per questo che il datore di lavoro ha come dovere e responsabilità quello di istituire una policy ove indicare quali comportamenti non possano essere effettuati, e tutelare così non solo i dipendenti o lui stesso, ma l'intero ecosistema aziendale [7].

Capitolo 2

Misure per la Protezione dei Dati Personali

Esiste una lunga lista di strumenti e tecnologie che gli addetti al settore possono utilizzare per elimiare, o quantomeno liminare, i problemi e le vulnerabilità a cui sono soggetti i dati personali. Questi stessi oggetti o pratiche possono essere valutate ed analizzate sotto vari punti di vista: validità temporale, utilizzi, peculiarità, vantaggi e svantaggi, e così via.

Una caratteristica suddivisione riguarda gli strumenti classificati come reattivi e proattivi: si tratta di valutare se l'oggetto in questione si occupa semplicemente di limitare i danni nel momento in cui l'esito dell'attacco è compiuto (strumetti reattivi), o di anticipare situazioni, disponendo quindi tutte le azioni possibili per evitare che ciò accada (strumenti proattivi).

L'importanza di questa caratterizzazione è determitata non solo dallo scopo di classificazione, ma anche dall'evoluzione storica e tecnologica del progresso: in linea temporale si è scelto di risolvere i problemi legati al trattamento dei dati personali prima utilizzando strumenti reattivi, come i *Privacy-Enhanching Tecnologies*, per poi - comprese le limitazioni - evolvere su strumenti proattivi *Privacy by Design*.

Nei paragrafi successivi, in considerazione delle intrinseche vulnerabilità della rete e della gestione delle informazioni personali e non (accesso, riservatezza, integrità autenticità) sara illustrate il complesso di contromisure tecnologie con i relativi punti di forza e debolezza.

2.1 PETs

Privacy-Enhancing Technologies è un sistema di misure ITC a tutela della privacy, il quale oltre ad avvalersi di contromisure tecnologiche standard (crittografia, controllo degli accessi e delle autorizzazioni, anonimato) ha come presupposto quello di eliminare o ridurre al minimo i dati personali, impedendo in tal modo elaborazioni inutili o indesiderate degli stessi, senza la perdita della funzionalità del sistema informativo [8]. Le PETs rappresentano un insieme di strumenti e tecnologie che, integrate in servizi ed applicazioni on-line, consentono agli utenti di proteggere le informazioni personali gestite da tali applicazioni.

2.1.1 Storia

La crezione avvenne nel 1995 quando le autorità di protezione dei dati tedesche ed olandesi, guidati dal lavoro del commissario Ann Cavoukian,pubblicarono uno studio così chiamato: *Privacy-Enhanching Tecnologies. A path to Anonymity.* Questo progetto esponeva come si potessero usare tecnologie e strumenti informatici per attivare misure preventive nella tutela dei dati personali, limitando al minimo l'utilizzo e la lavorazione degli stessi.

Il documento era poi basato sui FIPs, *fair information practise*, un insieme di principi riconosciuti in tutta la legislazione mondiale già negli anni '80, riassumibili in [10]:

- Minimizzazione dei dati utilizzati;
- Partecipazione degli utenti;
- Maggiore Sicurezza.

La prima applicazione commerciale basata su PETs fu sviluppata da ICL Netherland nel 1997; il sistema, costituito da un database ed una applicazione, serviva da gestionale in ambito sanitario. La sua caratteristica era determinata dall'utilizzo delle pseudo-identità; il paziente di un reparto era indicato nel database con uno pseudonimo, garantendone l'anonimato

rispetto agli addetti al reparto stesso. Queste persone non avevano accesso all'applicazione, riservata ai receptionists per operazioni di associazione identita-pseudonimo e viceversa; il sistema, oltre a possedere permessi speciali, utilizzava un protocollo di comunicazione criptata, garantendo maggior sicurezza [12].

2.1.2 I sette principi fondamentali

I PETs sono basati su questi principi [8]:

- Limitazione nella collezione di dati personali;
- Identificazione, autenticazione ed autorizzazione;
- Utilizzo di tecnologie standard per la protezione dei dati;
- Pseudo-identità;
- Crittografia;
- Biometria;
- Verificabilità.

Limitazione nella collezione di dati personali

Le informazioni raccolte ed utilizzate devono rispettare determinati requisiti: l'adeguatezza, la rilevanza e la necessità. Va infatti rispettato il principio cardine dei PETs, ovvero la limitazione dei dati trattati; si dovrà scegliere, di conseguenza, il minor numero di informazioni possibili data la loro importanza o la loro utilizzazione.

Identificazione/Autenticazione/Autorizzazione

Un buon sistema deve implementare queste tre specifiche; l'allegato B del Codice della Privacy, testo di riferimento nella normativa, prevede che solo i soggetti autorizzati possano procedere al trattamento dei dati personali. In questo modo è possibile costruire un sistema tale per cui a ciascuna figura venga riconosciuta dal sistema, che successivamente attribuisce la giusta autorizzazione di accesso.

Utilizzo di tecnologie standard per la protezione dei dati

Le PETs nascono come strumenti per la tutela delle informazioni personali; lo scopo principale risulta quindi quello di tutelare i soggetti interessati dal trattamento. La tutela, in questa visione, può essere garantita anche dall'anonimato. Questo ultimo punto non è visto come una celazione, bensì come una protezione d'identità del soggetto. Deve essere costituito un sistema tale per cui non sia possibile, con le informazioni a disposizione, ottenere una corrispondenza con un persona.

Pseudo-identità

E' il concetto cardine dei PETs ed è lo strumento che permette l'attuazione del punto precedente. E' quel meccanismo che cela le informazioni utili all' identificazione del soggetto reale con i suoi dati e costituisce l'idea di fondo del primo progetto commerciale creato da ICL.

Crittografia

Questo strumento garantisce un livello di segretezza durante il lavoro, e le sue potenzialità possono essere sfruttate durante le fasi di salvataggio, accesso, elaborazione e traferimento. Questo principio permette l'applicazione di alcuni principi sopra indicati; la tecnologia crittografica definisce politiche di controllo sugli accessi, oltre che proteggere le informazioni delicate.

Le tecniche messe a disposizione sono basate su sistemi di cifratura a chiave pubblica o privata, utilizzabili non solo in via diretta, bensì inserendoli all'interno di protocolli o di certificati.

Biometria

La rapida ascesa della biometria negli ultimi anni è data dal fatto che l'utilizzo, in combinazione con un altro strumento di identificazione, garantisce un alto livello di sicurezza. Infatti una password può essere recuperata, con tecniche più o meno semplici, mentre è molto difficile eludere il controllo di questo strumento. Iridi, flussi sanguigni, o altri particolari corporei sono unici e difficilmente riproducibili artificialmente; è la loro natura a determinare l'importanza degli strumenti nella garanzia un livello alto di sicurezza.

Verificabilità

Il Codice della Privacy prevede la presenza di autorità garanti che in qualunque momento possano verificare i dati raccolti e trattati; deve quindi esistere un meccanismo di tutela atto a mappare tutte le azioni intraprese, oltre alle informazioni stesse. Meccanismi di salvataggio di log oltre a copie delle stesse informazioni possono risultare utili a garantire questo principio.

2.1.3 Esempi di PETs

Esistono diverse tecnologie implementanti i principi delle PET come, ad esempio, i protocolli di cifratura (es. SSL, Secure Socket Layer v3, IPSec) o quelli di anonimato: generalmente si tratta di strumenti di crittografia o di sostegno alla filtrazione delle informazioni. Di seguito sono elencati i più rappresentativi oggetti hardware e software creati sui principi dei privacy-enhanced tecnologies.

Anonymizer

Gli *anonymizers*, chiamati anche *anonymizer proxies*, sono strumenti che permetto la non rintracciabilità delle azioni in rete. Si tratta di un proxy server che agisce da intermediario fra il PC e il resto del web, oscurando non solo indirizzo IP, ma anche il tipo di OS o software utilizzato [8]. Questi stessi strumenti vengono poi impiegati in casi più particolari, come l'elusione di censure nazionali o il non salvataggio della cronologia di navigazione, oppure per evitare che determinati servizi sfruttino informazioni private per scopi commerciali [13].

Gli anonimyzer fanno parte degli Anonymity Tools, PETs che provvedono a garantire sicurezza; i loro punti negivi riguardano la non capacità di celazione di informazioni di transizioni e il costo, spesso elevato. Altri esempi possono essere IPrivacy, Incogno SafeZone e .NetPassport; il primo, applicativo per dispositivi Apple®, attiva una modalità ospite la quale abilita solo determinate applicazioni od informazioni, in base a parametri scelti, garantendo così che sconosciuti non riescano ad ottenere dati sensibili, tramite l'individuazione della password [14].

Il secondo, applicativo lanciato dalla Incogno Corporation®, fornisce un meccanismo per l'acquisto online facendo in modo di prevenire la circolazione di dati sensibili quali dati delle carte di credito, nominativi, e così via [15].

P3P

Il P3P, conosciuta come *Platform for Privacy Preferences Project*, è un protocollo che permette ai siti web di dichiarare la destinazione d'uso delle informazioni raccolte durante la navigazione degli utilizzatori [16].

Molti siti web utilizzano pratiche di tracciamento dei propri clienti, ricavando così dati utili per creare annunci pubblicitari idonei. Il W3C, con l'intento di aumentare fiducia degli utenti e confidenza nel web, ha deciso di definire un working group per creare questo protocollo. Il punto di forza è determinato dall'utilizzo di XML schema per la definizione delle politiche; possedendo la caratteristica di essere *machine-readable*, tutti i browser sono in grado di abilitarlo ed attuarlo [11].

Ad oggi però, l'unico browser a gestirlo è Internet Explorer®, Mozilla ®ha cancellato il supporto nel 2000 e Google Chrome® *bypassa* le impostazione definite dagli utenti [17].

Questo strumento rientra all'interno dei *Policy Tools*, PET a sostegno degli utenti nel tutelare la propria privacy.

2.1.4 Utilizzo e Pregi

L'utilizzo maggiormente consolidato delle PETs è quello per la tutela dei dati dei clienti. Va inoltre valutato il tipo di dato sensibile trattato e il tipo di sicurezza applicabile od obbligatoriamente applicabile: uno strumento di alta protezione in ambiti non richiesti può produrre benefici, soprattutto se rivolto verso clienti, ma può comportare costi elevati ed alta specializzazione. Infatti i PETs richiedono investimenti in strumenti tecnici di medio-alto costo, corsi per l'ottenimento dei requisiti necessari all'utilizzo, e così via.

Ciò che si comprende è che, da una parte, questi strumenti costituiscono un costo, mentre dall'altra si ricava che il loro utilizzo non sostituisce strumenti già presenti. L'utilizzo di un anonymizer non preclude l'utilizzo di uno spyware, ad esempio, bensì favorisce l'unione di entrambi.

Il punto di forza lo si ricava dalla combinazione di componenti software ed hardware di varia natura, oltre al rispetto della legge, i cui PETs rappresentano un punto di focale contatto.

Altro pregio riguarda i metodi di acquisizione dei dati: i principi PET prevedono che essa sia fatta in modo tale che non vengano raccolti ed elaborati dati non *strettamente* necessari al compito richiesto. Questo provvede a ridurre la circolazione di informazioni, garantendo un livello di sicurezza maggiore.

2.1.5 Problemi

Ci sono diversi punti critici legati a questa tecnologia; idee, implementazioni, comportamenti o concezioni sono solo alcuni esempi [18].

In prima analisi una forte limitazione riguarda la concezione di creazione delle stesse tecnologie: i PETs nascono come strumenti per ridurre e limitare gli attacchi. La visione è limitata a misure per assicurare sicurezza, non a creare un sistema dove la protezione dei dati personali è insita nel concetto di privacy stessa. In sintesi si tratta di un approccio reattivo, dove gli utenti non possiedono il pieno utilizzo dello stesso, e non possono dunque vigilare sulla propria privacy con le azioni ritenute più corrette.

Diversi strumenti, per poter essere applicati, richiedono la modifica del sistema vigente, affichè risulti più affidabile, forte ed efficiente. Ad esempio, nel caso di sistemi simili a quello ospedaliero del ICL, il meccanismo di conversione richiede più tempo e risorse di calcolo per lavorare, e potrebbe comportare un'aumento della fragilità del sistema. Altro problema, riguardante gli Anonimyzer, rileva che se il servizio non è stato progettato per possibili utenti anonimi, o di default; questo consente che chiunque possa spacciarsi per una determinata persona ed utilizzare le credenziali di accesso della stessa.

Si ricava anche la necessità della ristrutturazione del meccanismo di identificazione sicura; troppo spesso basati su semplicità ed efficienze, essi richiedono oggi di essere più vicini al concetto di privacy, e sviluppare attorno ad essi una nuova idea. Alcune implementazioni, poi, sfruttano buchi della progettazione di applicazioni esistenti per aggiungere un livello di privacy,

ad esempio inserendo dati fittizi in campi destinati a trattenere identificatori univoci, a causa della mancanza di controllo appropriato da parte del sistema ricevente. Queste, come altre tecniche di sfruttamento di falle del sistema, sono simili alle tecniche utilizzate dagli hacker, spammer e programmatori di virus e possono ridurre seriamente l'affidabilità e la compatibilità dei software a cui fanno riferimento.

Altro punto di analisi riguarda gli utenti e la sicurezza; una delle prerogative dei PET è la *consegna* della responsabilità delle scelte agli utenti; ma cosa succede se gli utenti non sono in grado di gestirle o se non vogliono prendersene la responsabilità? Chi ha in mano la gestione di queste impostazioni? Quali sono quelle di default? Queste domande nascono dalla scarsa comprensione dei problemi di privacy nel pubblico in generale; molti la percepiscono solo nel momento in cui la perdono. La combinazione di questi due elementi porta i soggetti a non fidarsi della tecnologia, e quindi a non utilizzarla.

In sintesi, ci sono diversi punti che necessitano di revisione; deve maturare nella coscienza degli utilizzatori una nuova cosapevolezza sulle proprie informazioni. Vanno bilanciati gli interessi di tutela con la vita reale e con i bisogni dei singoli soggetti; va poi ristrutturato tutto l'impianto dei PET, risolvendo i problemi sopra-citati e permettendo la creazione di una nuova concezione. Sono stati per questo sviluppati i PETplus, tecnologie a tutela della privacy del tutto identici ai suoi predecessori, ma con una serie di peculiarità [10]:

- L'importanza della infrastruttura utilizzata;
- L'importanza della modellazione ed architettura scelta;
- L'importana del principio di fiducia e confidenzialità;

Si è infine compreso che doveva essere compiuta una completa ristrutturazione, portando ad un nuovo prodotto con caratteristiche e peculiarità ben diverse.

2.2 Privacy By Design

Privacy by Design rappresenta una serie di linee guida che affrontano il problema di trattazione dei dati personali all'interno della progettazione e sviluppo degli stessi sistemi, siano essi hardware che software. Questo approccio rappresenta un punto di vista forte; il principio consiste nel non delegare a soggetti terzi la gestione di tali informazioni tramite oggetti esterni, bensi si sceglie di affrontare questo problema direttamente all'interno della progettazione, utilizzando strumenti che si occupano di definire le politiche giuste di gestione, senza che lo sviluppatore se ne preoccupi.

2.2.1 Storia

Anni Novanta

La nascita del *PbD* può essere ricercata già negli anni novanta. In quel periodo diversi soggetti quali l'Unione Europea, Canada e USA dibattevano sulla possibilità di definire normative indicanti pratiche corrette sulla tutela della privacy. La direttiva europea 95/46/CE, fu considerata un buon punto di partenza; veniva infatti vista come un punto d'incontro fra la tutela dei diritti fondamentali e la libera circolazione di dati personali.

E' in questo periodo storico che nasce la volontà di definire uno strumento in grado di assicurare la tutela dei dati personali di ciascuno, cercando di non intralciare il progresso scientifico o di limitare l'iniziativa commerciale.

L'idea di partenza era quella di costruire la privacy all'interno degli strumenti, utilizzando come riferimento principi conosciuti da tempo, standard noti e linee guida rilevanti. Si decise di prendere in considerazione i *PETs*, con il preciso intento di evolverli ed adattarli alle esigenze indicate. Si scelse di considerare, poi, come punto cardine i *FIPPs (Fair Information Practises)*, dato che erano in grado di obbligare le organizzazioni a seguirle oltre a fornire indicazioni semplici sulla tutela delle informazioni personali.

I Fair Information Practises rappresentano una serie di linee guida redatte nel 1998 dalla American Federal Trade Commission [20]. La loro nascita risale però al 1973; il commissario del *US Advisory Committee on Automated Personal Data Systems* redasse un report chiamato *Records, Computers and*

the Rights of Citizens. In questo documento si analizzava la situazione di allora caratterizzata da una crescente elaborazione elettronica di dati personali, indicando, come soluzione, una serie di regole di sviluppo atte a, da un lato, garantire la privacy professionale, e dall'altro portare benefici nell'utilizzo in breve periodo [21]. All'interno del documento vi era anche indicata l'insieme dei principi FIPPs. Questi punti sono [22]:

- Trasparenza;
- Partecipazione individuale;
- Scopi Specifici;
- Minimizzazione dei Dati;
- Limitazione dell'utilizzo;
- Qualità dei dati ed Integrità;
- Sicurezza;
- Responsabilità e Controllo.

Durante il periodo di analisi ci si rese conto di come i *PETs* risultassero strumenti non più idonei per il compito scelto. Andava contruito un sistema più olistico ed integrato, costituito da pratiche di trattamento dati seguibili dalle organizzazioni, oltre ad un controllo più rigido e a strutture di responsabilità più solide.

Il Nuovo Millennio

Gli eventi e le conseguenze collegate a 11 Settembre 2001 furono tante, ma la più forte risultò il cambiamento di linea in materia di sicurezza interna. G. H. W. Bush firmò il USA Patriot Act, legge tuttora molto discussa la quale limita fortemente la privacy dei cittadini americani a favore di maggiori e migliori controlli attuabili da tutte le forze investigative del paese per limitare gli attentati terroristici. I cittadini accettarono questa normativa; per costoro era possibile sacrificare qualcosa per garantire pace e sicurezza non solo a loro, ma a tutta la comunità.

Questa concezione, ovvero sacrificare tutti gli obiettivi possibili a favore di uno soltanto - in questo caso la sicurezza nazionale - viene normalmente definito come *visione a somma-zero*.

Questo trend ebbe breve durata: già dopo un anno diverse agenzie governative di vari paesi si attivarono tramite iniziative e promulgazioni a favore di leggi sui dati personali e sulla privacy in generale. Furono coivolti sia settori privati che pubblici, cittadini comuni e commissari con l'idea che solo grazie all'aiuto di tutti si sarebbe costruita una legislazione atta a tutelare il diritto del singolo rispetto all'interesse di tutti.

Questa visione, contrapposta a quella precedente, si definisce a *somma-positiva*; l'obiettivo di tutelare i dati personali può concorrere assieme a quello della sicurezza nazionale.

Le esigenze che emersero dalle consultazioni furono le seguenti [19]:

- necessità di una normativa applicabile in vari ambiti, non solo quelli tradizionali;
- conversione degli strumenti tecnologici, adattandoli alle esigenze del contesto valutato;
- cambiamento dell'atteggiamento delle persone al controllo delle proprie informazioni;
- evoluzione degli organigrammi aziendali, includendo nuove figure professionali.

Un'altro principio assumeva importanza crescente: la fiducia. I consumatori ricercavano organizzazioni che utilizzassero i dati personali per fini pertinenti, trasformando quindi questa idea in punto di forza, soprattutto in ambito aziendale. Le aziende, per mantenere la propria quota di mercato o per aumentarla dovevano necessariamente investire in modo da istaurare fiducia nei possibili clienti.

Susseguirono, nel tempo, una serie di studi legati al campo informatico, sia per definire strumenti più idonei a garantire sicurezza - crittografia, biometria, strumenti di identificazione -, sia tool a sostegno dell'applicazione; ssempi di questi potrebbero essere *Privacy Diagnostic Tool*, strumenti

da usare in ambito aziendale per applicare principi rudimentali Privacy By Design in maniera corretta.

Nel 2005, una serie di *Information and Privacy Commisioner* canadesi collaborarono assieme per uno studio legato a come l'informatica avesse trasformato l'attività economica; i nuovi vantaggi economici raggiungibili, nuove tecniche di marketing e pratiche commeriali. Quello che emerse fu l'importanza che le **informazioni personali-identificabili** possedevano in quel momento. Si stava sviluppando un nuovo mercato commerciale, fatto di nuovi modelli aziendali e determitati problemi legati alla gestione dei PII, - raccolta, limitazione, eccetera -, necessitavano di una risposta.Non solo, emergeva la necessità di nuove figure professionali legate a questo ambito; persone con competenze sia giuridiche che informatiche che utilizzassero nuovi metodologie di lavoro.

Quello che produsse questo studio fu una serie di linee guida riguardanti diversi argomenti:

- Integrazione sicurezza e privacy;
- Considerazione aspetti legali, commerciali e comportamentali;
- Definire una figura di riferimento per la gestione della privacy aziendale;
- Utilizzo, ove possibile, di tecnologie esistenti;
- Costruzione di standard per la programmazione;

Conferenza di Gerusalemme

L'anno 2009 rappresenta un periodo cruciale per PbD; Ann Cavoukian pubblicò *7 Foundational Principles*, manifesto e raccolta di anni di studio e progetti. Vengono indicati i principi fondanti di questa visione, oltre ad un breve commento riguardante le discipline connesse. Dopo la sua pubblicazione i PbD assunsero un carattere di rilevanza in tutto il mondo, permettendo la sua applicazione obbligatoria negli stati Nord Americani. In ambito europeo la Commissione, valutata la necessità di una ristrutturazione del diritto della privacy decise di codificarlo all'interno del regolamento europeo.

Ulteriore riconoscimento venne raggiunto durante la conferenza di *Data Protection and Privacy Commissioner* di Gerusalemme del 2010. La risoluzione conteneva [23]:

> *... incoraggiamento all'adozione dei principi di Privacy By Design come parte di un meccanismo base di progettazione e un invito alla promozione di queste linee guida da parte dei Commissari, incentivando la codifica di essi all'interno delle legislazioni di competenza e promuovendo la ricerca attorno ad esse.*

Ad oggi, tutti gli Stati hanno codificato, o sono in procinto di farlo, i PbD all'interno della normativa di riferimento. Esistono figure professionali di riferimento a tutela della privacy in tutti gli stati ed sono presenti, infine, vari tool di utilizzo per l'applicazione corretta dei principi suddetti.

2.2.2 I Sette Principi Fondanti

Come sopra esposto, il Commissario Cavoukian nel 2009 ha indicato i principi cardine di questa visione, oltre agli strumenti utilizzabili. Rimane importante l'utilizzo di PETs evoluti, chiamati PETs Plus, adattati alle esigenze attuali in base ad analisi fatte precedentemente. I PbD sono visti come una combinazione di tre elementi fondamentali; tecnologie informatiche, pratiche commerciali corrette, infrastrutture di rete e progettazioni strutturali. I principi indicati sono [24]:

- Proatttivo e non reattivo: prevenire non correggere;
- Privacy come impostazione di default;
- Privacy incorporata nella progettazione;
- Massima funzionalità - valore positivo, non valore zero;
- Sicurezza ad intera protezione del ciclo di vita di un sistema;
- Visibilità e Trasparenza - Mantenere la trasparenza;
- Rispetto per la privacy dell'utente - Centralità dell'utente.

Proattivo e non Reattivo: Prevenire non Correggere

L'approccio caratteristico del PbD è la tempestività: secondo questa filosofia è molto più utile capire ed affrontare il problema, prima che si trasformi in danno reale e fattivo. Tutto ciò può essere applicato se: esiste la volontà di definire alti standard di privacy; esiste un coinvolgimento delle community o altre organizzazioni per la continua ricerca in materia; sono indicati metodi per l'identificazione e correzione di principi sbagliati legati alla privacy.

In ambito commerciale è facile capire come questo punto risulti cruciale: la prevenzione e l'anticipazione di possibili violazioni della privacy permettono di raggiungere un grado di soddisfazione alta nei clienti, oltre ad evitare costi inutili per un eventuale ripristino.

Privacy come impostazione di default

PbD cerca di realizzare il massimo livello di privacy garantendo che i dati personali siano automaticamente protetti in ogni sistema informatico, qualunque esso sia; in questo modo ogni persona manterrà il grado di riservatezza senza dover compiere nessuna azione. Ciò può essere compiuto se si rispettano i principi FIPs di scopi specifici, utilizzo e limitazione nella collezione dei dati, minimizzazione dei dati.

Per gli utenti questo rappresenta un punto imporante, essendo i primi attori nella gestione delel proprie informazioni.

Privacy incorporata nella Progettazione

L'intendo dei PbD è quello di integrarsi in fase di progettazione nel sistema di sviluppo dell'oggetto; questo non deve risultare un impedimento, un modo per far diminuire le funzionalità, bensì un nuovo modo di concepire lo sviluppo, bilanciando le esigenze di privacy con le funzionalità del sistema stesso. Questo deve essere fatto per integrare la realtà con la progettazione dei sistemi, siano essi IT o commerciali; utilizzando framework di sviluppo e standard sarà possibile aiutare gli sviluppatori a creare il loro applicativo in maniera più aderente possibile ai principi PbD.

Questo principio sottolinea come il concetto di privacy sia qualcosa di ineludibile ai giorni nostri; ma la soluzione ottimale si ottiene solo quando

è essa stessa intrinseca e nativa nei sistemi, in modo tale che siano loro a gestirla nel modo corretto.

Massima Funzionalità - Valore positivo, non valore zero

PbD punta ad indicare come l'approccio somma-positiva risulti quello ottimale nel trattamento dei dati personali; non serve infatti sacrificare tutti gli obiettivi a discapito di uno solo, è possibile tutelarli tutti tramite compromessi.

Questo risulta essere uno dei principi fondamentali: non si vuole definire una gara per trovare quale, fra sicurezza e privacy, sia l'obiettivo da seguire. E' possibile curare entrambi, attraverso soluzioni creative che puntino all'innovazione.

Sicurezza ad intera protezione del ciclo vitale di un sistema

Cosiderato il punto tre di questa lista, è possibile assicurare sicurezza all'intero ciclo di vita dei dati contenuti. La scelta di inserirlo come elemento primario rispetto alla progettazione permette la protezione delle informazioni in modo adeguato. PbD assicura, così, un'intera e sicura gestione delle informazioni.

Tutto questo è realizzato solo se si rispetta il principio FIP sicurezza, integrandola nel sistema ed applicandolo.

Visibilità e trasparenza - Mantenere la trasparenza

Data la natura dei PdD principles, è fondamentale tenere traccia di tutte la azioni compiute nello sviluppo di un determinato software per diverse ragioni: la prima riguarda un possibile controllo che chi commissiona il sistema ritiene importante effettuare. Se un ente terzo verifica le operazioni è possibile verificare la presenza di errori o mancanze, e persone esterne possono informarsi, prima di affidare i propri dati all'ente aziendale in questione. Altro punto, che non è strettamente legato al PbD prevedere che nel caso di sostituzione, permanente o momentanea, dei soggetti addetti allo sviluppo sia possibile, per i sostituti, comprendere in breve tempo e continuare il lavoro affidato.

Questo principio di responsabilità, trasparenza e rispetto si eredita dai FIPs. Il primo punto riguarda l'insieme dei dati raccolti e di come, su di essi, ricada un obbligo di tutela: quindi tutte le operazioni e procedure devono essere documentate, in modo tale che chi necessiti possa controllarla. Ne consegue che tutte queste informazioni possano essere visualizzate da persone esterne, costruendo quindi un meccanismo di trasparenza.

Rispetto per la privacy dell'utente - Centralità dell'utente

Quest'ultimo concetto risulta essere il più importante: al di là di ogni esigenza, quella dell'utente deve essere sempre la più importante. Tutti gli operatori devono considerare come primari gli interessi degli individui, centrando gli obiettivi di tutela della privacy con interventi di default di facile utilizzo. Questa idea è basata su una serie di principi FIPs quali accesso, consenso, accuratezza e conformità: sono tutte pratiche molto importanti, servono ad istaurare quel rapporto di fiducia fra gli utenti e le organizzazioni. I primi, compreso come i loro dati personali saranno trattati, saranno più rassicurati permettendo un crescente numero di nuovi potenziali clienti.

2.2.3 Vantaggi nell'utilizzo di Privacy by Design

Si comprende facilmente come l'applicazione di queste linee guida rappresenti un vantaggio importante sia in fase di sviluppo che in ambito aziendale; la gestione di tematiche complesse viene fatta all'interno degli stessi strumenti, eliminando costi notevoli. Non solo, un punto fortemente vantaggioso per le aziende riguarda la non volontà di limitazione dello sviluppo, permettendo una creazione libera, senza impedimenti.

L'utente in PbD assume quella posizione centrale necessaria come evoluzione rispetto ai PETs: si costruisce un sistema basato sulla fiducia, requisito fondamentale per l'attività aziendale.

Relazioni economiche basate su fiducia non producono solo un ritorno economico, ma un sentimento tale da garantire una catena di consumatori fedeli in grado di modificare il mercato.

La centralità dell'utente non è più una prospettiva, ma un'idea concreta, implementata da politiche user-centric per la diffusione dei dati personali; il

soggetto, tramite i vari strumenti a suo utilizzo, potrà giungere ad un pieno utilizzo del sistema, così come indicato nei principi fondanti.

Il trattamento di dati personali diventa così costruito su politiche che permettano agli utenti una facile comprensione, rafforzando il ruolo centralizzato dell'utente; la gestione delle informazioni non sarà più obbligatoriamente fatta dagli utenti, ma saranno gli utilizzatori delle stesse, per primi, a creare politiche tali da non richiedere il convolgimento di quest'ultimi nella normale gestione.

L'idea portante del PbD è quella di costruire un mondo dove tutto potesse coesistere in modo bilanciato, dove tutti potessero guadagnare e nessuno perdere - come esplica la filosofia somma-positiva. Ed è proprio questo a farne un punto di forza; tutti traggono vantaggio nell'utilizzo e nell'applicazione.

Capitolo 3

Quadro Normativo Italiano Ed Europeo

Questo capitolo espliterà le norme riguardante il trattamento dei dati personali a livello nazionale, con il decreto legislativo 196/2003, e a livello europeo, con la direttiva 46 del 1995 e con la proposta di regolamento 11 del 2012 in esame al Parlamento Europeo.

3.1 Storia della Normativa Italiana

Il primo atto normativo in materia di trattamento di dati corrisponde alla legge n.675 del 31 dicembre 1996, *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali.* Questo atto era stato introdotto in ottemperanza ai trattati di Schengen e alla direttiva 46 emanata dalla comunità europea nel 1995 [25].

Dopo questa data si sono succeduti una serie di decreti legislativi il cui compito era quello di redimire piccole controversie come la notifica del trattamento dei dati personali[1], la salvaguardia della vita privata in ambito giornalistico[2], eccetera. Gli interventi normativi si sono moltiplicati nel tempo

[1] D.lgs. n.255 del 28 luglio 1997, *Disposizioni integrative e correttive della Leggen. 675 del 31 dicembre 1996, in materia di notificazione dei trattamenti di dati personali, a norma dell'art. 1, comma 1, lettera f), Legge n. 676 del 31 dicembre 1996.*

[2] D.lgs. n. 171 del 13/05/1998, *Disposizioni in materia di tutela della vita privata nel settore delle telecomunicazioni, in attuazione della direttiva 97/66/CE del Parlamento*

e, insieme all'evoluzione della tecnologia, si è richiesto la creazione di un vero e proprio codice, chiamato Codice della Privacy[3]; il testo rappresenta una raccolta delle norme sancite dal decreto legislativo n. 255 e di tutti i decreti prodotti in seguito.

La Comunità Europea, nel 2010, ha condotto una serie di studi per valutare se la normativa in materia di trattamento dei dati risultasse ancora coerente; i vari studi hanno fatto emergere la necessità di una nuova normativa europea, ancora in fase di approvazione.

3.2 Direttiva 95/46/CE

La Direttiva 46 non è altro che la conversione degli Accordi di Schengen; patto stipulato fra una serie di Stati, non necessariamente appartenenti all'Unione Europea, questo patto rappresenta un passo importante nella costituizione dell'Unione. Il suo fine consisteva nella determinazione di regole comuni per il combattimento di crimine e controllo delle frontiere [26].

Il fine della Direttiva era quello di garantire i cittadini degli stati aderenti i diritti fondamentali durante l'esecuzione di qualunque operazione sui dati da parte di un soggetto raccoglitore, definito titolare; il soggetto a cui appartenevano queste informazioni assumeva il titolo di interessato.

Il testo è suddiviso in varie parti a seconda del tipo di trattamento effettuato - generale o particolare -, e delle azioni compibili dall'interessato per la propria tutela o per il sistema sanzionatorio.

3.2.1 Principi Giuridici

A livello giuridico è importante ricordare non solo la determinazione del diritto di riservatezza, o di personalità, bensì l'introduzione del consenso informato tramite un'informativa obbligatoria. Prima che il soggetto fornisca i dati personali, egli stesso deve fornire il consenso, leggendo l'informativa in cui, per legge, sono esplicati non solo i dati del titolare, ma anche i fini del trattamento e l'utilizzo dei dati fatti.Deve poi essere sempre possibile all'interessato l'accesso, la verifica e la cancellazione dei dati.

europeo e del Consiglio, ed in tema di attività giornalistica (modificato dal d.lg. 467/2001).

[3]D. lgs. 30 giugno 2003, n. 196

I dati sensibili possono essere trattati solo previa autorizzazione dal Garante della Privacy, figura terza nominata in ogni singolo stato il cui compito è quello di verificare l'applicazione della legge.

3.2.2 Principi Tecnici

Per quanto concerne il livello tecnico, il codice prevedere, all'articolo 17 comma 1:

> [...] il responsabile del trattamento deve attuare misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali [...].
>
> Tali misure devono garantire, tenuto conto delle attuali conoscenze in materia e dei costi dell'applicazione, un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere.

La definizione generica di **livello di sicurezza appropriato** indica come sia compito del titolare, o dell'incaricato in caso di presenza, di valutare il progresso tecnologico e scegliere quale siano le tecnologie più corrette a salvaguardia della banca dati creata. Ai fini di prova poi, come indicato nello stesso articolo al comma 4, è necessario indicare per iscritto tutte le informazioni riguardanti la protezione dei dati e le misure scelte.

In base all'articolo 27, la Commissione e i vari Stati incoraggiano la definizione e l'utilizzo di codici di condotta atti a semplificare la comprensione e l'applicazione del testo.

3.2.3 Conversione in Legge

L'applicazione della Direttiva si deve, in Italia, alla legge n.675 del 31 dicembre 1996. Il testo di quest'ultima è stato arricchitto con norme attuative, atte a esplicare meglio concetti astratti del testo europeo.

All'articolo 15 si introduce il concetto di misure minime di sicurezza e della loro trasformazione in misure adeguate a partire dal biennio della data di approvazione della suddetta legge. Non solo; si indica la necessità, a

cadenza bimestrale, di definire ulteriori regolamenti per aggiornare le misure tecniche al passo evolutivo in base all'esperienza maturata.

Una ulteriore specifica in merito si ottiene con il Regolamento emanato dal Presidente Della Repubblica, il n.318 del 28 luglio 1999, *recante norme per l'individuazione delle misure di sicurezza minime per il trattamento dei dati personali.*

A differenza di tutti i testi precedenti la sua tecnicità, data dalla specifica applicazione di misure quali parole chiave per l'accesso dei dati [4], o codici identificativi[5], rende il testo vincolante nella progettazione di sistemi per la gestione del trattamento dei dati personali.

Quelli sopra sono solo alcuni esempi; si indica l'obbligatorietà di strumenti informatici contro il rischio di intrusione, pena la violazione del codice penale come da articolo 615 *quinquies* dello stesso. Altro punto di valutazione riguarda l'impiego di strumenti di memorizzazione; la loro riusabilità viene valutata in base alla capacità di mantenimento dei dati al loro interno. Se non si è in grado di cancellare permanentemente le informazioni sopra indicate si deve procedere alla distruzione.

L'articolo 5 del Regolamento introduce il concetto di autorizzazione al lavoro: ogni singolo individuo deve poter eseguire solo e soltanto le azione strettamente necessarie a svolgere il proprio lavoro. Si limitano, quindi, competenze e postazioni di lavoro - l'accesso a due o più macchine in contemporanea è vietato -.

L'articolo successivo introduce l'obbligatorietà deel documento programmatico di sicurezza dei dati: si tratta di un report recante informazioni quali criteri tecnici ed organizzativi per la protezione delle aree e il controllo di accesso dei soggetti, criteri tecnici per l'assicurazione dell'integrità dei dati, misure atte a garantire la sicurezza nella trasmissione dei dati e la definizione di un piano di formazione per tutto lo staff tecnico incaricato del trattamento dei dati. La cadenza di produzione del suddetto documento è annuale e va integrato con controlli a cadenza regolare per garantire tutti i punti sopra indicati siano rispettati.

[4] art.2, comma 1, lettera a, D.P.d.R. del 28 luglio 1999, n.318.
[5] art.4, comma 1, lettera a

3.3 Decreto L.vo 196/2003

3.3.1 Storia

L'evoluzione tecnologica ha comportato la produzione di numerosi decreti attuativi e regolamenti legati alla legge 675 del 1996. In conseguenza a ciò, nel 2001, il Parlamento Italiano, tramite Legge Delega, concedette al Governo la creazione una nuova normativa in materia di trattamento di dati, che tenga conto delle leggi precedenti e della Direttiva 2002/58/CE in merito alla tutela dei dati personali nel settore delle telecomunicazioni.

Il decreto legislativo del 30 giugno 2003, n.196 è il risultato di questo processo di aggregazione ed aggiornamento ed è tuttora la normativa vigente in Italia.

3.3.2 Testo

I principi di misure minime di sicurezza e misure adeguate rimangono invariati; i due articoli che li riguardano sono sostanzialmente identici rispetto alla legge 675/1996. La parte nuova riguarda le misure attuate dai fornitori di comunicazione e all'introduzione di un allegato alla legge recante le misure minime adottate.

Per quanto riguarda i provider o altri soggetti incaricati di fornire servizi di comunicazione, su di loro ricadono obblighi di sicurezza sulle comunicazioni, ove la protezione dei dati lo richieda. Nell'articolo 32 si indica come su questi soggetti ricada l'obbligo di utilizzare tutti gli strumenti atti a garantire la sicurezza nelle sudddette reti, e di comunicare agli utilizzatori casi di possibile violazione del canale stesso indicando quali ambiti non ricadono nel controllo del fornitore.

L'articolo 34 esplica le tecnologie consentite per il trattamento dei dati stessi:

- Autenticazione informatica;
- Procedure di gestione delle credenziali di autenticazione;
- Sistema di autorizzazione;
- Aggiornamento periodico delle figure atte al trattamento;

- Protezione di dati e strumenti rispetto a possibili trattamenti illeciti, accessi non consentiti e programmi non autorizzati;
- Mantenimento di copie di sicurezza, procedure di ripristino di dati e sistemi;
- Produzione ed aggiornamento del Documento Programmatico sulla Sicurezza;
- Tecniche di cifratura o codici identificativi per determitati trattamenti di dati quali, ad esempio, salute o vita sessuale nei casi previsti.

Il decreto legislativo prevede poi che queste misure siano coordinate con allegato B della legge suddetta. Questo testo, *Disciplinare tecnico in materia di misure minime di sicurezza*, esplica le misure minime a carico alle figure che si occupano del trattamento dei dati e di chi costruisce sistemi di gestione di questi. Nel Codice è previsto poi l'aggiornamento periodico del suddetto allegato, tramite decreto del Ministro di Grazia e Giustizia.

L'allegato B contiene requisiti come la lunghezza delle chiavi di autenticazione, - stabilite nel massimo della lunghezza prevista dal programma partendo da un minimo di otto -, la cancellazione di chiavi non utilizzate per più di sei mesi, la cancellazione di profili di autorizzazione non necessari in maniera periodica.

L'articolo 19 ribadisce l'obbligatorietà di stesura ed aggiornamento annuale del Documento Programmatico, includendo nel suddetto le seguenti informazioni:

- L'elenco dei trattamenti effettuati;
- La distribuzione dei compiti all'interno della struttura;
- L'analisi dei rischi sulle banche dati;
- L'insieme delle misure adottate per garantire l'integrità e la disponibilità die dati, nonchè il tipo di protezione effettuata;
- L'insieme dei criteri e delle modalità di rispristino dei dati a seguito di una ipotetica distruzione o danneggiamento degli stessi;

- L'insieme di attività formative da effettuare all'interno della struttura;
- L'elenco delle misure minime adottate.

Da notare che questo stesso articolo è stato abrogato tramite il Decreto Legge del 9 febbraio 2012, n.5, *recante disposizioni urgenti in materia di semplificazione e sviluppo.*

Una serie di articoli, che vanno dal 20 al 24, indicano misure supplementari applicate nel trattamento di dati sensibili o giudiziari; tutti volgono ad elimare l'accesso abusivo a queste informazioni fornendo specifiche riguardanti l'utilizzo, ad esempio, di supporti rimovibili, la definizione di idonee misure per il ripristino dell'accesso alle banche dati in caso di danneggiamento o distruzione delle stesse.

3.4 Proposta di Regolamento Europeo 2012/0011

3.4.1 Premesse

Come indicato nell'introduzione, nel 2010 si è ritenuto necessario, da parte del Parlamento Europeo una revisione della direttiva 46 per gestire meglio le seguenti problematiche [27]:

- Gestire l'impatto con le nuove tecnologie;
- Insufficiente armonizzazione fra le norme di protezione degli stati membri;
- Rivedere le norme sul trasferimento dei dati;
- Rafforzare il ruolo delle autorità di protezione dei dati;
- Definire uno strumento globale applicabile a tutti i settori e politiche.

Il progresso scientifico ha consentito la creazione ed utilizzo di strumenti lontanamente immaginabili anni prima, strumenti tali a produrre e gestire grandi quantità di dati personali. Il fine ultimo della commissione europea, nella produzione di questo nuovo testo, è stato quello di creare un clima di fiducia nel mercato on-line: la non fiducia produce frenate

sul commercio elettronico, portando ad un possibile arresto dell'innovazione tecnologica [28].

Per questo, a partire Programma di Stoccolma - atto normativo dettante l'agenda per l'Unione europea in materia di giustizia, libertà e sicurezza per il periodo 2010-2014 - è partito l'iter per la creazione di un nuovo quadro giuridico: l'idea maturata con le varie consultazioni fatte è stata quella di definire un quadro giuridico più ampio rispetto alla direttiva precedente, in modo da limitare le problematiche sopra citate, mantenendo fermi i principi cardine tra cui la neutralità del profilo tecnologico scelto.

Si sono susseguite una serie di comunicazioni e consultazioni dove hanno partecipato non solo i parlamentari europei, bensi cittadini, organizzazioni pubbliche e private. Contributi importanti sono giunti anche dal Gruppo di lavoro Articolo 29 - commissione indipendente creata per compiti consultivi -, che ha apportato modifiche importanti riguardanti, ad esempio, la definizione della politica da utilizzare sui cookies e sugli strumenti biometrici.

Il Regolamento è ancora in fase di discussione al Parlamento Europeo; dopo aver ricevuto parere favorevole da varie commissioni il testo è rimasto bloccato per diversi mesi. Alcuni Stati Europei, fra cui la Germania, trovavano il testo troppo morbido nella definizione di diritti fondamentali. Il 4 dicembre, i ministri di giustizia dell'Unione hanno trovato un'accordo di massima e si attende l'imminente approvazione.

3.4.2 Testo

Il regolamento 11/2012 ha l'obiettivo di toccare la quasi, se non tutta, totalità della casistica possibile in materia di trattamento dei dati personali.

Per natura delle sue caratteristiche, poi, rappresenta un atto avente valore di legge nello stato di applicazione, non necessitando di ulteriori atti di approvazione negli Stati Membri. Di conseguenza il testo è notevole e contiene atti specifici su diversi punti; l'analisi proposta, in sintesi, riguarda solamente i punti considerati rilevanti per il percorso intrapreso all'interno di questa Tesi.

Trasparenza, fiducia ed armonizzazione

Il principio di trasparenza - art.11, comma 1 -, introdotto come punto cardine nel trattamento dei dati personali, assume un valore importante; solo se l'interessato comprenderà in modo chiaro i suoi diritti e doveri sarà in grado di assumere azioni chiare e precise. Per questo il legislatore definisce l'obbligatorietà di comunicazioni con informazioni precise - art.14 -, sistemi di accesso e modifica semplici, come indicato dall'articolo 15 e 16 del testo. Altro punto di rilevanza riguarda l'istituzione di specifiche certificazioni utilizzabili dalle organizzazioni in modo tale da stabilire quel principio di fiducia invocato nelle intenzioni iniziali. Il legislatore europeo incoraggiare l'utilizzo di strumenti, identificabili subito dall'interessato, in modo tale da fargli capire quale sia il suo livello di affidabilità e garantire il livello di trasparenza richiesto dall'articolo 11.

Diritto all'oblio

Il diritto all'oblio, sancito dall'articolo 17, riguarda una cancellazione definitiva di informazioni non più utili al fine del trattamento o non più pertinenti, o raccolte in un momento di minore età. Il testo prevede l'obbligatorietà per qualunque organizzazione di eliminare, sotto richiesta dell'interessato, in maniera permanente codeste informazioni.

Portabilità

La Commissione ha deciso di sancire, all'interno del testo, il principio di portabilità dei dati, ovvero la distribuzione dei dati da parte del titolare all'interessato; questo vale solo quando questi dati siano in formato elettronico e la loro struttura sia di *comune* uso. Questo permetterebbe all'interessato non solo il controllo sulle proprie informazioni, bensì una redistribuzione delle stesse ad altre organizzzazioni.

Privacy By Design

L'articolo 23 del Regolamento recita:

> 1) Al momento di determinare i mezzi del trattamento e all'atto del trattamento stesso, il responsabile del trattamento, tenuto conto dell'evoluzione tecnica e dei costi di attuazione, mette in atto adeguate misure e procedure tecniche e organizzative in modo tale che il trattamento sia conforme al presente regolamento e assicuri la tutela dei diritti dell'interessato.
>
> 2) Il responsabile del trattamento mette in atto meccanismi per garantire che siano trattati, di default, solo i dati personali necessari per ciascuna finalità specifica del trattamento e che, in particolare, la quantità dei dati raccolti e la durata della loro conservazione non vadano oltre il minimo necessario per le finalità perseguite. In particolare detti meccanismi garantiscono che, di default, non siano resi accessibili dati personali a un numero indefinito di persone.
>
> [...]

Mentre la prima parte - riprendendo il concetto di misure adeguate esposto nella Direttiva Europea 45/95 - espone le misure indicate come minime affichè siano tutelati i diritti dell'interessato, il secondo comma indica l'obbligatorietà di utilizzo dei principi Privacy by Design, così come indicati nel capitolo precedente. Questo principio viene rafforzato nell'articolo 30 comma 3; trattando di sicurezza dei dati il legislatore indica:

> *Alla Commissione è conferito il potere di adottare atti delegati[...] al fine di precisare i criteri e le condizioni concernenti le misure tecniche e organizzative [...], compresa la determinazione di ciò che costituisce evoluzione tecnica, per settori specifici e in specifiche situazioni di trattamento dei dati, in particolare tenuto conto degli sviluppi tecnologici e delle soluzioni per la protezione fin dalla progettazione e per la protezione di default, [...].*

Responsabile della Protezione dei Dati

L'articolo 22 del Regolamento indica l'obbligatorietà di un responsabile della protezione dei dati:

> *Il responsabile del trattamento adotta politiche e attua misure adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati personali effettuato è conforme al presente regolamento. Le misure [...] comprendono, in particolare: la designazione di un responsabile della protezione dei dati, [...].*

Questa figura professionale rappresenta l'oggetto di analisi di questa tesi e ad essa sarà dedicato uno spazione nella Parte II. Possiamo indicare comunque che i suoi compiti ed obblighi sono indicati nel testo tramite gli articoli 35, 36 e 37.

Parte II

Implementazione

Capitolo 4

Buone Prassi Implementative di Privacy by Design

In questo capitolo analizzeremo come, concretamente, si sviluppano i sette principi di Privacy By Design precedentemente elencati, evidenziandone gli attori coinvolti e l'implementazione sviluppando, infine, per ciascun principio PbD la concreta applicazione.

Per meglio evidenziare i requisiti e le caratteristiche Privacy by Design, viene introdotta la descrizione delle funzionalità dei più importanti framework ed applicazioni le cui specifiche possono connotarsi nel Privacy by Design sia per progettazione, che per servizi forniti.

4.1 Gruppo di lavoro

Il modello pensato e concepito in base ai principi PbD è dinamico, ma con ruoli ben definiti [29]. Il gruppo di lavoro è formato da varie figure professionali che interagiscono nello sviluppo dei sistemi informativi di gestione: sviluppatori, analisti, Privacy Officer o Data Protection Officer. Gli analisti definiscono le Privacy Policies aziendali, linee guida di riferimento per il trattamento dei dati, gli sviluppatori implementano i Privacy Requirements, requisiti necessari allo svolgimento delle specifiche. Compito del DPO o PO sarà quello di definire, verificare e concorrere a mantenere i principi di privacy da applicare nel progetto. Un costante contatto fra sviluppatori ed

i responsabili dei dati, poi, favorirà la corretta applicazione dei principi fino al completamento, oltre ad aiutare lo sviluppo del sistema per rispettare al meglio le norme giuridiche di riferimento.

I Principi Privacy By Design sono codificati, di default, nelle Privacy Policies Aziendali e la loro combinazione con pratiche e processi a supporto di questa materia definiscono un background di lavoro sempre presente.

La creazione delle Privacy Policies è strettamente legata ai sette principi cardine del PbD: ciascuno di essi definisce linee guida per ogni figura del gruppo di lavoro, portando a quella visione olistica a somma-positiva necessaria per creare un sistema vicino che tuteli il più possibile le informazioni personali.

4.2 Applicazione Concreta dei PbD principles

4.2.1 Proattivo e non reattivo: prevenire non correggere

La tempestività nell'agire prima ancora che il problema possa sorgere caratterizza questo principio: la prevenzione di problemi permette di agire ancora prima che essi si sviluppino, favorendo la protezione delle informazioni.

Il monitoraggio costante del progetto, per valutare il rispetto delle Privacy Policies aziendali, insieme alla promozione di strumenti di largo utilizzano comportanto la creazione di sistemi facilmente mantenibile e modificabile, grazie al feedback delle comunità. Le politiche scelte devono dunque essere forti, consistenti e all'avanguardia e sostenute da investimenti ingenti.

Questo tipo di leadership, definita da un approccio esecutivo ma guidato permette la rapida espansione della cultura della privacy in tutta l'azienda, garantendo un miglior successo. Figura importante, in questo ambito, è il Privacy Officer o il Data Protection Officer; in essi è racchiuso il successo della corretta attuazione delle politiche della privacy e del loro successo.

La proattività richiesta in questo caso può essere colta tramite l'analisi delle tecnologie in fase di sviluppo o di ultima uscita; solo una comprensione anticipata dei rischi legati all'oggetto permettono la creazione di contromisure applicabili a tutela delle informazioni. Strumenti a sostegno di queste

analisi sono i Privacy Impact Assessment, o PIA; il loro compito è quello di identificare possibili rischi legati ai dati personali nel progetto e di ridurli al minimo possibile. Molto utile in fase di sviluppo, il suo utilizzo è legato anche al processamento più efficiente dei dati; la sua modularità lo rende uno strumento utilizzato non solo da CPO o sviluppatori, bensì da un team composto da membri dei due gruppi indicati assieme a: membri del marketing, addetti alla sicurezza, rappresentanti del mondo IT, e così via.

4.2.2 Privacy come impostazione di default

Concetti fondanti di questo principio sono: privacy-protective e data minimization. Il primo esplica la visione secondo cui la progettazione di un sistema IT deve partire senza alcuna collezione di PII; nel caso in cui siano richieste informazioni personali deve sussistere uno specifico e convincente scopo per raccoglierle.

Il secondo punto impone la raccolta solo di dati strettamente necessari; questo comporta un minor rischio di compromissione di informazioni inutili allo scopo - notizie non presenti nel database non possono essere visionate, modificate, e così via. Inoltre, grazie alla potenza di calcolo dei moderni computer, è possibile ottenere informazioni in maniera rapida, utilizzando dati personali già memorizzati nella raccolta, evitando memorizzazioni inutili e pericolose.

La possibile raccolta di dati personali genera un problema di uso e memorizzazione degli stessi, che viene risolto applicando il principio FIPs di uso limitato; combinando tecnologie e misure organizzative, pratiche di scomposizione di dati con diversi accessi e ruoli si ottiene un sistema di difficile violazione.

In ambito organizzativo i compiti vengono suddivisi fra vari soggetti; la responsabilità di applicare il principio di data minimization ricade su progettisti e sviluppatori, mentre agli analisti si richiede l'ottemperanza del principio di privacy-protective, in coerenza delle specifiche richieste da chi ha commissionato il sistema. Ai programmi di sviluppo spetta il compito di applicare tutte le tecniche per garantire il principio di uso limitato.

4.2.3 Privacy incorporata nella progettazione

Privacy by Design sostiene l'importanza di considerare la privacy e la sua gestione non come fattori di seconda importanza, bensì come elementi cardine durante tutto il ciclo di vita del software; la sua trattazione rappresenta un elemento chiave per rompere con la vecchia metodologia di lavoro, più legata a conciliare, con piena funzionalità e senza compensazione, gli interessi e obiettivi del sistema.

E' richiesto quindi un processo di ristrutturazione che non coinvolge solo l'ambito aziendale, ma tutti gli attori che si avvicendano durante la fase di progettazione, sviluppo ed implementazione. Quello a cui si vuole giungere è la definizione di nuovi atti regolamentari, buone prassi implementative, framework le cui specifiche sono quelle di attribuire ai dati personali la giusta tutela e protezione; una nuova visione sfaccettata che valutando le aspettative dei clienti e consumatori, problemi e requisiti di privacy, produce gli strumenti per affrontare la realtà.

Ogni attore ha un proprio compito da svolgere: gli sviluppatori, ad esempio, hanno il compito di considerare gli aspetti legati ai dati personali durante tutto lo sviluppo, introducendo, ove possibile, nuovi meccanismi innovativi per migliorare l'analisi. Ai proprietari delle applicazioni e programmi spetta il compito di introdurre *Privacy Risk Assessment* come strumento di analisi dei rischi in qualunque momento della fase di progettazione; si tratta di un insieme di tools che hanno il compito di identificare obiettivi e scopi da tutelare a livello aziendale, in modo da poterli valutare e poi determinare quelli che realmente saranno le politiche di privacy aziendali.

Ai legislatori spetta il compito di definire una serie di atti normativi, come leggi, regolamenti, framework, e così via.

4.2.4 Massima funzionalità - Valore positivo, non valore zero

Ciò che caratterizza i principi PbD rispetto alle visioni antecedenti è proprio il concetto di somma a valore positivo; si tratta di una visione in cui su una serie di obiettivi non ne prevale uno solo, ma tutti insieme concorrono alla positiva finalizzazione degli obiettivi. Si tratta di un pensiero olistico

dove, in questo caso, privacy non viene subordinato ad altri interessi legittimi quali, ad esempio, sicurezza ed efficienza.

Quello a cui si vuole giungere, è la dimostrazione della coesistenza di due principi fondamentali: privacy e sicurezza. La creazione di modelli non invasivi nella gestione di dati sensibili, ovvero modelli che mantengono solo le informazioni strettamente necessarie e ne definiscono metodi di utilizzo, rappresenta un punto di svolta nell'applicazione di questo principio nel ciclo di sviluppo del software.

Compito del gruppo dirigente è la promozione di questa visione, in cui molteplici e legittimi interessi possono e devono coesistere. Ai progettisti e sviluppatori ricade l'onere di ricercare, creare ed utilizzare soluzioni innovative per realizzare tutte le funzionalità richieste nel caso di elaborazione. Ai PO (Privacy Officer) o ai DPO (Data Protection Officer) spetta il compito di aiutare tutte le figure per meglio capire ed gestire tutti gli interessi, siano essi divergenti o similari tra loro.

4.2.5 Sicurezza dell'intero ciclo di vita di un sistema

Sicurezza è il concetto chiave per privacy; senza di essa non è possibile attribuire nessuna responsabilità e nessun diritto. Solo con l'applicazione dei principi legati alla sicurezza, ed in particolare quelli legati all'uso della crittografia, è possibile assicurare la gestione delle informazioni in maniera corretta per tutto il ciclo di utilizzo delle stesse.

E' importante attribuire ai possessori di dati personali e sensibili la responsabilità degli stessi; in questo modo saranno essi stessi ad utilizzare e ad applicare consapevolmente ed applicare non solo i principi della sicurezza in generale, - integrità, disponibilità e confidenzialità -, bensì tutti gli standard internazionali universalmente riconosciuti.

Per quanto appena detto, la parte più delicata ricade sugli sviluppatori e progettisti software, il cui compito è quello di applicare le metodologie di sicurezza al fine di eliminare, o quanto meno ridurre, le preoccupazioni legate a compromissione di dati; parliamo non solo di furti o perdite, ma anche di cancellazioni complete o parziali di informazioni conservate in vari dispositivi, siano essi di memoria secondaria o supporti esterni.

Tutte queste metodologie vanno poi integrate con i dispositivi ed i flussi di lavoro in maniera automatica ed trasparente; questo, tra gli altri, è il compito che viene genericamente attribuito ai Privacy Officer, dato che la loro non è soltanto una figura di consulenza.

4.2.6 Visibilità e trasparenza - Mantenere la trasparenza

La trasparenza rappresenta una caratteristica rilevante nella creazione o aggiornamento di un progetto: se vengono rispettati gli obiettivi dichiarati all'utente, se i documenti utilizzati sono chiari, se le politiche di controllo sono precise sarà possibile istaurare quel grado di fiducia ed affidabilità necessari a permettere ai soggetti interessati di potersi fidare dell'azienda.

Compito di tutti i membri del gruppo di lavoro è quello di dimostrare l'applicazione efficace di tutte le azioni necessarie, soprattutto in caso di violazione o contestazione da parti terze. La continua richiesta di aderenza da parte delle organizzazioni rispetto a standard di controllo per le informazioni personali ha richiesto la definizione di protocolli, metodologie, regolamenti uguali per tutti definibili solo con una legislazione comune in merito.

Per questo, gruppi di lavoro indipendenti si stanno organizzando per definire standard di responsabilità applicabili in ambito aziendale, in cui sono incluse anche metodologie di controllo, standard di valutazione e tecniche implementative. Quello che si vuole sottolineare è che gli utenti devono essere a conoscenza di tutte le informazioni personali conivolte nel sistema o nel processi siano portate all'attenzione dei clienti in maniera rapida e processabile.

Compito degli sviluppatori e dei progettisti di sistemi sarà quello di definire metodologie semplici di accesso alle informazioni delle persone, assieme a quelle riguardanti i dati aziendali. Ai Privacy Officer o Data Protection Officer è quello di creare, reperire, impiegare paradigmi semplici nella stesura di documenti leggibili dagli utenti, in modo da rendere facile la comprensione. Ai regolatori spetta, infine, il compito di definire strumenti di controllo tali da permettere anche agli utenti di poterli comprendere ed utilizzare.

4.2.7 Rispetto per la privacy degli utenti - Centralità dell'utente

Il concetto di centralità dell'utente può essere visto sotto due punti di vista: il primo definibile come il diritto di controllo delle proprie informazioni, ed il secondo visto come sistema costrutito sulla visione degli utenti, e quindi delle loro esigienze. Anche se i due aspetti possono essere visti come in contraddizione, PbD li valuta entrambi corretti e li sostiene, indicandoli come necessari; un sistema non deve solo essere costruito per gli utenti, ma deve essere pensato e strutturato per essi.

Misure per garantire trasparenza, ottenimento del consenso informato al trattamento dei dati, definzione di diritti di accesso e correzione sono alcuni esempi di cosa si intenda per sistema costruito per utenti. Per quanto riguarda la strutturazione di sistemi per gli utenti si possono citare la definizione di meccanismi di privacy e preferenze fatta in modo semplice, funzionale e persistente nel tempo.

Gli utenti devono aver modo di gestire le informazioni a loro riguardanti in maniera facile e veloce e possibilmente permettendo di definire meccanismi di default di alto profilo, mentre la gestione delle compromissioni dei dati deve essere fatta in maniera tempestiva e completa.

Infine, considerare il ruolo degli utenti come soggetti attivi ed attenti permette l'introduzione di uno dei meccanismi di controllo più efficaci rispetto ad abusi ed altre misure. La rivoluzione informatica ha costruito utenti consapevoli ed esperti nell'utilizzo di tecnologie e strumenti: persone capaci di muoversi in maniera più veloce ed attenta. E' per questo che deve essere costruito un sistema che permetta agli utenti di gestire le informazioni nella maniera che loro ritengono opportuna.

Il compito di occuparsi di garantire questo principio spetta agli sviluppatori e progettisti, che dovranno definire politiche di gestione della privacy di default di alto profilo, nuovi meccanismi di notificazione, oltre a rendere persistenti le preferenze degli utenti. Sono richiesti nuovi metodi di accesso ai dati legati all'utente e all'azienda, in modo da instaurare nell'interessato i principi migliori per decidere le azioni da voler compiere.

Capitolo 5

Ricognizione di framework o Applicazioni implementativi Privacy By Design

Questo capitolo sarà dedicato ad illustrare alcuni dei framework o sistemi che implementano alcuni principi Privacy by Design. La letteratura in questo ambito è varia e legata principalmente all'ambito universitario americano; questo è dovuto al fatto che i principi sono stati codificati per primo in Canada e, successivamente, in America. Il trattamento dei dati personali e la gestione della privacy ricalcano quindi il modello americano, più permissivo di quello europeo, sia considerando quello attuale che quello futuro. La descrizione delle funzionalità di queste applicazioni ha come finalità quella di ulteriormente descrivere requisiti e caratteristiche del Privacy by Design.

5.1 Piwik

Piwik è un *Web Analytics Platform* rilasciato in licenza *GNU General Public License* nel 2008; rappresenta la prosecuzione del progetto phpMyVisites e con esso condivide il linguaggio di sviluppo, PHP [30].

Si presenta come alternativa ai più conosciuti *Google Analytics* ed è utilizzato da *Wikipedia.de* e da *privacybydesign.ca*; è disponibile in oltre cin-

quanta lingue ed è impiegato in oltre un milione di siti web nel mondo, in centocinquanta paesi [31].

5.1.1 Caratteristiche

Come indicato precedentemente, Piwik è sviluppato in linguaggio PHP e possiede diversi punti di forza: l'alta personalizzazione del software è implementata dalla possibilità di estensione dello stesso, tramite istallazione e rimozione di plugin provenienti da un marketplace contente software con diverse licenze di utilizzo [33].

L'interfaccia è costruita in modo tale da permettere il trascinamento ed il rilascio di widget (elementi con interfaccia grafica) in maniera totalmente personalizzata, creando la visualizzazione in base alle esigenze richieste.

Il recupero delle informazioni dei visitatori del sito web avviene in tempo reale, permettendo quasi istantaneamente la visualizzazione di informazioni legate alla geolocalizzazione, alla provenienza del traffico, al tracciamento di file in download, e così via.

La semplicità dei widget permette una rapida comprensione ed utilizzazione dello strumento: le informazioni recuperate sono visualizzate tramite immagini e diagrammi, permettendo un rapido apprendimento. E' possibile gestire sia file in download se presenti, sia campagne di tracking in pochi e semplici passaggi.

5.1.2 Vantaggi e criticità

Piwik è considerata una delle soluzioni di analisi più protettive della privacy presenti in circolazione; è provato che molti software o servizi di *Web Analytics* si approprino delle informazioni legate ai visitatori dei siti web o web app in analisi, utilizzandole poi per vari scopi. In questo caso ciò non avviene in quanto le informazioni rimangono memorizzate sui database MySQL degli stessi; i log o i report vengono costruiti ed inviati direttamente agli indirizzi di riferimento, senza passare quindi per i server del software[34].

Piwik include poi una serie di plugin di default configurati in modalità *privacy-compliance*: uno fra questi è il servizio *Anonymise IP Addresses*. Il servizio permette il salvataggio degli indirizzi IP all'interno dei database

MySQL in maniera tale da oscurare parte dell'indirizzo stesso - da uno a tre byte dell'indirizzo, sia per la modalità IPV4 che per quella IPV6.

E' possibile configurare il servizio in maniera tale da cancellare automaticamente i file di log; creato inizialmente come plugin per database MySQL di grandezza ridotta, ha assunto connotazioni di tutela della privacy dato che permette la cancellazione di file fino a quelli giornalieri.

La tecnologia *DoNotTrack* è implementata all'interno di Piwik: si tratta dell'utilizzazione dal parte dell'utente di un particolare header HTTP costruito in modo tale da permettere, nel caso di implementazione da parte del web browser di utilizzo, la non tracciabilità dello stesso nel momento in cui visita il sito web [35]. Sebbene sia ancora in fase di standardizzazione da parte del W3C, molti browser già supportano la tecnologia ed è possibile quindi applicarla. Di default Piwik rispetta la scelta degli utenti, e di conseguenza anche questa tecnologia. Nella gestione dei cookies è possibile settare Piwik in maniera tale da disattivare la creazione degli stessi per condurre analisi: di default questa non è un'opzione attiva ma configurabile dall'utente.

Alla luce delle caratteristiche appena indicate, Piwik implementa due dei sette principi fondanti della dottrina Privacy by Design:

- Privacy come impostazione di default;
- Rispetto per la privacy dell'utente, Centralità dell'utente.

5.2 OpenPDS

OpenPDS, o *Personal Data Stores* è un progetto sviluppato da MIT HUMAN DYNAMICS GROUP volto a garantire e tutelare la privacy delle informazioni personali, viste in ambito di metadati [36].

OpenPDS integra e centralizza la gestione dei dati personali, definendo uno strumento, un gestore di dati personali, semplice e facile da usare: tutti i servizi devono ricorrere ad esso se necessitano di metadati per svolgere le proprie specifiche. Da sottolineare il fattore che non è possibile estrarre informazioni dal raccoglitore, ma è possibile usarle, appoggiandosi a moduli secondari, per produrre azioni. Il fine ultimo è quello di definire un luogo centralizzato sicuro dove raccogliere i metadati, come ad esempio un server

personale od una macchina virtuale, a cui un servizio software indipendente può rivolgersi.

Altra caratteristica è la portabilità: OpenPDS ha cercato di creare un servizio portabile; l'utilizzo del database CouchDB e della struttura dei documenti JSON permette la definizione di uno standard applicabile in altri sistemi. L'utente potrà così scegliere il servizio più adatto alle proprie esigenze, portando i dati con se [37].

5.2.1 Composizione

OpenPDS è composto da due parti: back-end, formato da un database che colleziona i vari metadata relativi all'utente, e il front-end. Quest'ultimo rappresenta la parte più innovativa del sistema: si tratta di trasformare il problema di anonimato in uno legato alla sicurezza. Sostanzialmente si tratta di un meccanismo che permette la consultazione dei dati senza che vengano portati via dal database ed utilizzati per altri fini.

Front-End: Safe Answers Modules

La parte di front-end è pensata con l'obiettivo di impedire che operazioni non autorizzate siano eseguite sui metadati. Sul database insistono politiche di accesso che filtrano le informazioni, mediante moduli client (Safe Answers Modules) che in autonomia elaborano le informazioni sui metadati.

Ogni modulo viene registrato al database come utente, ottenendo così un codice identificativo univoco utilizzato per il controllo degli accessi; oltre a questo vanno poi aggiunte le politiche di permissioning utilizzate dai moduli SA insieme al meccanismo di controllo di accesso degli utenti in Django. Framework di alto livello scritto in Pyton, Django implementa sia autorizzazione che autenticazione utilizzando sistemi personalizzabili di hashing per password, sistemi di accesso sia per utenti che per gruppi, sistemi di controllo degli accessi o di risorse particolari.

Le comunicazioni fra l'applicazione e il modulo SA corrispondente avviene tramite connessione cifrata SSL da 256 bits e si sta procedendo alla separazione fra il meccanismo di accesso e PDS stesso, utilizzando il protocolo OAuth 1.0, usato anche in Django.

La parte di front-end costituisce anche il punto di controllo per l'utente rispetto all'applicazione: infatti nei vari moduli è possibili per quest'ultimo stabilire quali siano le informazioni accessibili e quali no. Normalmente questo meccasimo viene effettuato dai dispositivi su cui si utilizzano le applicazioni, ma talune implementazioni permettono anche la personalizzazione tramite web browser.

Si sta procedendo alla creazione di librerie comuni che permettano una creazione semplificata di moduli SA, permettendo agli sviluppatori di concentrare i maggiori sforzi sulle applicazioni stesse.

Back-end: Database

Il database è di tipo CouchDB, un modello non relazionale di tipo noSQL: utilizza il formato JSON per il salvataggio delle informazioni ed il linguaggio JavaScript per l'interrogazione dello stesso, usando MapReduce attraverso CouchDB-Views, HTTP come API ed una serie di strumenti per permettere il salvataggio di documenti corretti.

Questo sistema non sfrutta il concetto di schema e tabella tipico dei modelli in commercio: ogni contenitore, chiamato documento, non è altro che una scatola contenente chiavi e valori associati. Ciascun documento differisce dagli altri, sia per la natura eterogenea degli stessi, sia per le informazioni contenenti.

Ciascuno Modulo SafeAnswers accedera al database unificato, ma ciascuno utilizzando una propria chiave in modo tale da permettere la visione specifica delle sole informazioni consultabili dall'applicazione. Lo stesso database può imporre l'accesso in base ai tipi di informazioni richieste, tempi di accesso o raccolta, ed eventuali altri parametri di controllo.

L'intero progetto è stato redatto in linguaggi Pyton e JavaScript ed è distribuito in licenza open source MIT: ad oggi è stata sviluppata la parte del database e del modulo di gestione. Non sono ancora stati sviluppati moduli SA per testare il funzionamento completo, ma esiste un modulo di prova applicabile come test di demo.

5.2.2 Funzionamento

Quando una applicazione ha bisogno di compiere azioni collegate a metadati degli utenti, è la stessa a contattare il servizio PDS dell'utente, utilizzando come interfaccia il proprio modulo SafeAnswers. Ogni applicazione, per interagire con PDS, deve possedere un proprio modulo creato per ricevere le informazioni dal database ed elaborare le richieste valutanto le stesse.

Il modulo SA si occupa di elaborare la richiesta, accedendo alla parte di back-end e richiedendo i dati necessari. L'accesso è regolato dall'utente che usa PDS, che può autorizzare o meno la consultazione di talune informazioni.

Al termine della richiesta il modulo stesso provvederà ad inviare il risultato all'applicazione, che lo utilizzerà per compiere le azioni richieste.

Nel momento di istallazione dell'applicazione PDS-aware è necessario concedere alla stessa i diritti di accesso agli strumenti necessari, - accesso alla rete internet, GPS -: al primo avvio sarà l'applicazione stessa a richiedere l'indirizzo URI PDS riferito al soggetto e verrà poi installato, se l'utente lo autorizza, il modulo SA di riferimento dell'applicazione, permettendo poi la configurazione dei metadata accessibili o meno.

5.2.3 Punti di forza e criticità

OpenPDS può considerarsi PbD compliant poiché considera principalmente la privacy come una forma di tutela per l'utente, il quale è primario attore nel controllo e nella gestione del sistema informativo specificatamente pensato e dedicato alla raccolta e alla gestione sicura ed affidabile di dati personali.

Per il tipo di problematica e per la soluzione utilizzata si riscontrano problemi legati alla sicurezza, alla natura distribuita della soluzione, e di come questi fattori impattano le prestazioni.

In primo luogo, la natura distribuita della applicazione sviluppata può portare a problemi nella gestione della risposta; quando il tempo di ricezione di risposta è dominato dall'elaborazione del database vanno studiati meccanismi per eliminare la latenza.

Questa criticità è un problema aperto connesso in particolare ad alcune tipologie di informazioni che richiedono meccanismi di sicurezza più forti

rispetto a quelli classici: più risulta sicuro il sistema usato, più esso influisce sulle prestazioni. Oggetto di particolare attenzione e di miglioramento a quindi considerato molto attentamente è il meccanismo di criptazione usato nelle comunicazioni fra il database ed i moduli SA, per dati personali finanziari o sensibili per i quali un necessario meccanismi di cifratura molto forte non pregiudichi l'acquisizione e la celere fruizione delle informazioni.

5.3 HIDE

HIDE, *Integrated System for Health Information DE-identification*, è un framework Django scritto in Phyton con database CouchDB che viene distribuito con una licenza free software MIT, ed è utilizzabile sia su sistemi Unix-like che Windows-based [38]. Il suo fine è quello di produrre la de-identificazione di documenti legati a dati sanitari: dato in input un documento contenente dati etorogenei di varia natura, si ottiene in input una visione anonimizzata dello stesso, dove i dati sono completamente scollegati dagli interessati.

Il sistema è basato sull'impianto normativo americano, caratterizzato da *Health Insurance Portability and Accountability Act*: si tratta di una legge approvata dal governo Clinton nel 1996 il cui scopo consiste nel «*migliorare la portabilità e la continuità di copertura assicurativa sanitaria nei mercati di gruppo e individuali, per combattere sprechi, frodi e abusi in assicurazione sanitaria e la fornitura di assistenza sanitaria, per promuovere l'uso di conti di risparmio medici, per migliorare l'accesso ai servizi di assistenza a lungo termine e la copertura, per semplificare la gestione di assicurazione sanitaria, e per altri scopi*» [39]. Oltre a questo, il HIPAA - abbreviazione della legge - è famoso per aver introdotto la standardizzazione dei sistemi di gestione di informazioni legate alla salute; in particolare tutti coloro che intendono procedere al trattamento di dati sanitari o affini deve rispettare le norme contenute nel testo.

Lo scenario di utilizzo è il seguente: si consideri, ad esempio, un istituto di ricerca che voglia produrre una rete di condivisione di dati accessibili a chiunque abbia l'autorizzazione ad accedere al servizio. Le informazioni raccolte durante il processo di ricerca devono, per legge, non permettere la

diretta identificazione delle stesse con il soggetto; così come avviene nelle ricerche statistiche, dove i dati raccolti non hanno collegamento diretto con le persone che le hanno prodotte, lo stesso principio deve essere applicato nello scenario.

5.3.1 Tipologie di Dati

Per comprendere appieno sia il funzionamento del framework, sia le tecniche utilizzate per implementarlo, è necessario comprendere i tipi di dati che si utilizzano all'interno del sistema [40].

I *Unique identifiers*, o idenficatori unici, rappresentano quelle categorie di attributi atti ad identificare in maniera univoca il soggetto in questione. Questo genere di attributi viene soppresso dal programma, dato che per la normativa di riferimento non possono essere trattenuti.

I *quasi-identifiers*, o quasi-identificatori, rappresentano invece una piccola porzione delle informazioni che combinate assieme ad altri attributi esterni possono permettere l'identificazione del soggetto. Esempi in questo caso possono essere l'età, il sesso, il luogo di provenienza, e così via: questo genere di informazioni sarà trattato con particolari tecniche che verranno illustrate successivamente in modo tale da eliminare qualunque collegamento con l'esterno.

Infine, i *sensitive attributes*, o identificatori sensibili, rappresentano tutti quei valori tali che non dovrebbero permettere l'associazione diretta delle informazioni con i possessori; si tratta genericamente dei dati sensibili, ed in particolare di dati sanitari.

5.3.2 Struttura del Framework

Il framework è composto da una serie di componenti chiave che interagiscono fra loro per trasformare un documento contenente informazioni eterogenee in uno schema di anonimizzazione avanzato.

Il primo componente che si applica è il *data linking*; considerato che non è possibile procedere ad una relazione uno ad uno fra soggetto e tupla, - è possibile che un paziente abbia più una corrispondenza all'interno dei dati -, è necessario procedere alla connessione degli attributi rilevanti per ogni entità,

o struttura contenente i dati, al fine di creare *person-centric representation* dei dati stessi.

Successivamente, si procede all'estrazione delle informazioni identificative o a quelle sensibili non necessarie allo svolgimento del compito, - i dati sanitari rientrano nella categoria dei dati sensibili -. Mentre alcune sono facilmente rincracciabili, - età, nominativo, codice identificativo -, altre possono essere celate o tradotte in modo diverso all'interno del testo. Il componente *identifying and sensitive information extraction* procede alla cancellazione dei suddetti dati dal testo.

Queste due operazioni, eseguite più volte, produrranno una strutturata *identifier view*; si tratta di una grande tabella, ciascuna delle quali contiene tuple formate da più informazioni - quelle consensite dal HIPAA -, sulla quale vanno applicate tecniche avanzate di anonimizzazione. Va ricordato che la rimozione di talune informazioni non comporta l'automatica de-identificazione del soggetto; alcuni dati, quali l'età, il sesso, o il codice postale, non sono considerati come identificativi o sensibili, ma comportano, se analizzati insieme, possibili associazioni dirette.

5.3.3 Processo di Anonimizzazione

Il processo di de-identificazione dei dati viene fatto attraverso l'attuazione di due operazioni applicate in due tecniche. Le operazioni riguardano la generalizzazione o la rimozione delle informazioni, mentre le tecniche di anonimizzazione possono essere: k-anonimizzazione e l-diversificazione.

Il primo fornisce un modello in cui nessun record individuale possa essere univocamente identificato all'interno di un gruppo di k tuple, valutando i quasi identificatori. Considerato l'insieme totate delle tuple T, una classe di equivalenza corrisponde ad un gruppo di elementi ove i quasi-identificatori assumono valori identici. L'insieme T risulterà k-anonimizzato quando ogni tupla della classe di equivalenza ha dimensione almeno k.

La seconda, ovvero la tecnica di l-diversificazione, consiste nella presenza di almeno l identificatori sensibili identici all'interno della classe di equivalenza, in modo da evitare che le informazioni omogenee rivelino informazioni atte a ricoscere il gruppo.

Queste tecniche sono state elaborate dalla dottoressa Latanya Sweeney, docente di *Government and Technology in Residence* presso l'università di Harvard e *Chief Technology Officer, also called the Chief Technologist* presso *U.S. Federal Trade Commission (FTC)*[41].

5.3.4 Processo di Estrazione Attributi

Il processo di estrazione di attributi identificativi e sensibili da dati non strutturati rientra all'interno dei *Named Entity Recognition Problem*, o NER; si tratta di problemi secondari di estrazione di informazioni che cerca di individuare e classificare gli elementi nel testo in categorie predefinite [42]. Esistono due categorie di risoluzione: la prima sfrutta le tecniche basate su grammatiche o regole provenienti da linguaggi, mentre la seconda utilizza approcci all'apprendimento linguistico. Entrambi richiedono tempi di eleborazione troppo lunghi per poter permettere l'utilizzo dei dati da parte degli utenti.

Si è quindi ricorso ad un approccio di apprendimento statitistico, in particolare *a Conditional Random Fields-based named entity recognizer* per estrarre attributi sensibili ed identificativi. Il campo condizionale casuale, o CRF, è un avanzato modello probabilistico discriminante che prende in ingresso una sequenza di token dal testo dove ogni token possiede una serie di funzionalità basate sulla sequenza. Dato un token dalla sequenza CRF calcola le probabilità della possibile etichettatura e sceglie quella con massima probabilità. La probabilità di ciascuna etichetta è una funzione del set di funzioni associate a tale token.

Il punto chiave è rapprensentato dal set di funzionalità: in questo caso i creatori hanno selezionato come caratteristice la presenza di caratteri speciali, di numeri - nel caso di token -, la parola precedente e quella successiva, ed altri punti; tutte le caratteristiche scelte derivano dallo studio di sistemi NER biometrici.

Il processo, infine, è composto da una serie di passaggi:

1. Un software di codifica usato per tutti i tipi di dati, compresi quelli sensibili ed identificativi;

2. Un classificatore basato su CFR utilizzato per classificare termini dal testo in più classi;

3. Un insieme di strategie di pre e post elaborazione dei dati, usando approcci iterattivi, per estrarre caratteristiche dei dati al testo per il classificatore e per alimentare il processo di correzione e retagging del software.

5.3.5 Punti di forza e criticità

HIDE risolve uno dei problemi più sentiti dalla dottrina Privacy By Design, ovvero quello della de-identificazione: la possibilità di dissociazione delle informazioni rispetto agli interessati comporta un livello di tutela di questi ultimi molto alto.

Come avviene da molti anni in paesi quali Paesi Bassi, Belgio e Canada, questi strumenti sono impiegati in larga scala anche in ambito sanitario pubblico, quali ospedali e studi medici.

La rimozione o la generalizzazione di talune informazioni sensibili riduce notevolmente il possibile utilizzo delle stesse per scopi malevoli o, più semplicemente, non autorizzati. E' però necessario garantire accesso alle stesse, non solo per fini personali, bensì per pubblica utilità; questa implementazione rispetta quindi uno dei principi Privacy By Design: *Massima funzionalità – Valore positivo, non valore zero.*

Capitolo 6

Figura di Privacy Officer

Il Privacy Officer concorre a garantire che i diritti degli interessati dei dati personali siano rispettati; nata in America negli anni novanta ha origini antiche.

In Europa questa figura viene definita come Data Protection Officer, ovvero responsabile della protezione dei dati personali; è prevista dal regolamento CE 45/2001, *concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati.* Questo capitolo analizzerà questa figura, mostrando compiti e competenze, sia quelle attuali che quelle future indicate nel regolamento in fase di approvazione 2012/0011.

6.1 Creazione ed Evoluzione Storica della figura

La comparsa della figura di Privacy Officer, - PO in breve -, risale al 1970 in Assia, uno dei sedici stati federali tedeschi.

Data l'approvazione della prima legge americana di tutela alla privacy del 1960, lo stato tedesco decise di promulgare una legge in materia definendo, fra le tante cose, la figura di *Datenschutzbeauftragter*, Responsabile della protezione dei dati [43]. Nel 1977 fu promulgata dallo stato centrale tedesco la prima legge sulla protezione dei dati personali rendendo di fatto obbligatorio l'assunzione, sotto deteminati requisiti, di queste figure in ambito aziendale [44].

Il PO o Chief Privacy Officer, - CPO in breve, utilizzato in ambito aziendale americano -, ha assunto la connotazione attuale negli anni novanta.

Nel 1999 la società AllAdvantage assunse l'avvocato R. E. Church come Privacy Officer; le crescenti preoccupazioni dei consumatori americani riguardanti il trattamento spettato ai dati personali portò le aziende ad integrare nel proprio staff dirigenziale figure che, occupandosi delle informazioni dei consumatori, infondessero fiducia negl stessi.

Nel nuovo millennio il numero di PO assunti nelle grandi aziende fù in rapido aumento, anche grazie alla normativa europea approvata che indicava l'obbligatorietà, sotto determinati canoni, di assunzione di queste figure. Successivamente iniziarono a nascere le prime società professionali e le prime associazioni di categoria.

In Italia l'arrivo di questa figura è stato tardo: nonostante la legislazione europea lo richieda, l'assunzione di Privacy Officers all'interno di contesti aziendali non obbligatori è ancora bassa. Questo può essere spiegato dal fatto che nel Paese non è radicata una concezione di tutela delle informazioni; l'introduzione di questa figura non è stata fatta per fini strategici o tutelativi verso i consumatori, bensì tutto il sistema di tutela del trattamento dei dati è stato visto come un costo, un atto burocratico, un impiego di tempo e denaro inutile. Di conseguenza, l'investimento aziendale ha assunto in molti casi, come scopo principale, quello di evitare sanzioni da parte del Garante della Privacy; soluzioni lowcost, PO scelti fra persone con scarse competenze sono solo alcuni esempi di questa visione.

6.2 Obbligatorietà di assunzione e competenze richieste

Al momento attuale, il testo normativo di riferimento è il regolamento CE 45/2001. Per quanto riguarda le competenze richieste il testo, all'articolo 24 comma due si legge:

> *Il responsabile della protezione dei dati è scelto in funzione delle sue qualità personali e professionali e, in particolare, delle sue conoscenze specifiche in materia di protezione dei dati.*

La proposta di regolamento 2012/0011 è, in questi ambiti, molto più precisa; l'articolo 35 dello stesso esplica sia le competenze richieste, che l'obbligatorietà di assunzione. Per quest'ultimo si individuano tre casi:

- Qualora il trattamento dei dati sia compiuto da un'autorità od organismo pubblico;
- Qualora il trattamento sia effettuato da un'impresa con più di 250 dipendenti;
- Qualora la natura, l'oggetto o le finalità del trattamento richiedano un controllo regolare e sistematico degli interessati.[1]

Il testo specifica poi la possibilità per l'ente pubblico di accorpamento dell'incarico verso una sola persona e si indica, poi, la possibilità di assunzione di un responsabile per la protezione dei dati anche nei casi non previsti dalla lista sopra indicata[2].

Per quanto concerne le competenze richieste, il suddetto articolo al comma cinque specifica molto dettagliatamente che il responsabile deve essere scelto in base alle qualità professionali, analizzando sia la conoscenza normativa, sia per le capacità di adempiere ai compiti attribuiti, e quindi alle conoscenze tecniche aquisite.

Circa la durata del mandato, entrambi i testi normativi indicano come mandato minimo quello di due anni, con possibile rinnovamento. Mentre il primo atto risulta più specifico sulla durata complessiva dello stesso - al massimo dieci anni -, il secondo non indica una durata massima.

Entrambi i testi attribuiscono la facoltà di destituzione del Responsabile solo quando egli non soddisfi più le condizioni richieste nell'esercizio delle sue funzioni [3].

[1] art. 35, comma 1, COM(2012) 11 final del 25 gennaio 2012, *concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)*

[2] art. 35 comma commi 2, 3, 4, COM(2012) 11 final del 25 gennaio 2012

[3] art. 35, comma 7, COM(2012) 11 final del 25 gennaio 2012 e art. 24 comma 4 Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio del 18 dicembre 2000

6.3 Compiti Attribuiti e Posizione Aziendale

Sia il regolamento europeo in vigore che quello in attesa di approvazione contengono al loro interno una lista dettagliata di compiti attribuiti al responsabile della protezione dei dati personali. Entrambi convergono sulla funzione consultiva e di controllo affidata a questa figura: viene esplicitamente indicato come su costui ricada l'obbligo di collaborare con i responsabili, informandoli su obblighi e diritti a loro attribuiti, e vigilando che il regolamento sia rispettato in ogni sua parte. E' compito del responsabile collaborare con le autorità europee competenti, rispondendo a richieste ricevute dalle stesse e notificare nuovi trattamenti.

Il Regolamento in fase di attuazione è però più specifico su alcuni punti: al responsabile del trattamento viene attribuita una funzione vigilativa sull'attuazione del regolamento, con particolare interesse sulla protezione fin dalla progettazione - Privacy By Design -, sulla protezione dei dati, sulla formazione del personale, e così via. Va poi aggiunto un ulteriore controllo; viene infatti richiesto al responsabile di vigilare sulla redazione della valutazione d'impatto effettuata dal titolare, oltre che a tutti i documenti richiesti dal regolamento stesso.

La figura che emerge è quella di un tecnico sia giuridico, che informatico; un osservatore molto attento che funge da consulente sulle tematiche più complesse, soprattutto in ambito tecnico. L'articolo 36 del futuro Regolamento indica come il responsabile della protezione dei dati comunichi le sue analisi direttamente ai superiori gerarchici del titolare, ponendolo, così, a livello dirigenziale.

Al responsabile della protezione dei dati viene garantita, da entrambi i testi, l'indipendenza e l'autonomia nello svolgimento del proprio lavoro: il titolare deve fornire tutto il supporto possibile, sia a livello logistico che umano, e deve assicurare il pronto e completo coinvolgimento del responsabile nel lavoro.

Al PO spettano i seguenti compiti, in base all'articolo 37 del COM 2012/0011:

- Informare e consigliare il responsabile del trattamento o l'incaricat del trattamento in merito agli obblighi derivanti dal presente regolamento

e conservare la documentazione relativa a tale attività e alle risposte ricevute;

- sorvegliare l'attuazione e l'applicazione delle politiche del responsabile del trattamento o dell'incaricato del trattamenot in materia di protezione dei dati perosnali, compresi l'attribuzione delle responsabilità, la formazione del personale che partecipa ai trattamtni e gli audit connessi;

- sorvegliare l'attuazione e l'applicazione del presente regolamento, con particolare riguardo ar requisiti concernenti la protezione fin dalla progettazione, la protezione di default, la sicurezza dei dati, l'informazione dell'interessato e le richieste degli interessati di esercitare i diritti riconosciuti dal presente regolamento;

- garantire la conservazione della documentazione di cui all'articolo 28;

- controllare che le violazioni dei dati personali siano documentate, notificate e comunicate ai sensi degli artt. 31 e 32;

- controllare che il responsabile del trattamento o l'incaricato del trattamento effettui la valutazoine d'impatto sulla protezione dei dati e richieda l'autorizzazione preventiva o la consultazione preventiva nei casi previsti dagli artt. 33 e 34;

- controllare che sia dato seguito alle richieste dell'autorità di controllo e, nell'ambito delle sue competenze, cooperare con l'autorità di controllo di propria iniziativa o su sua richiesta;

- fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento e, se del caso, consultare l'autorità di controllo di propria iniziativa.

Si espone in seguito il funzioni-gramma aziendale che include il PO.

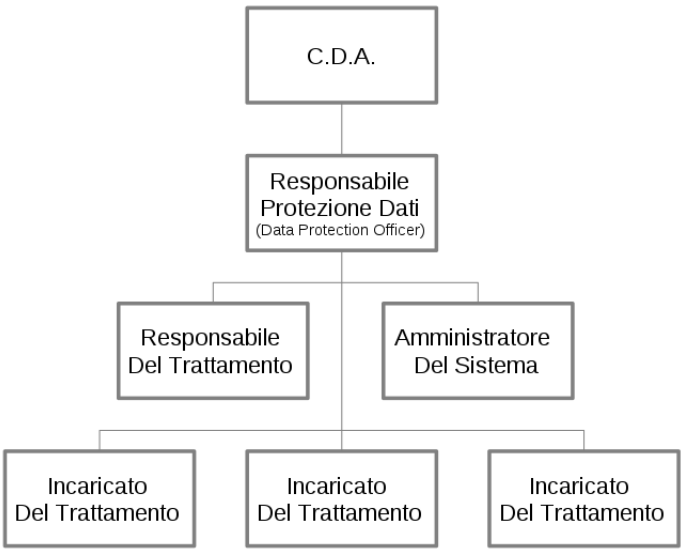

Figura 1: Funzionigramma aziendale che include il PO.

Parte III

Sicurezza del Trattamento dei dati con modalità elettroniche: analisi dei rischi in un contesto aziendale e comparazione tra PET e PbD

Capitolo 7

Sistema di Gestione della Sicurezza delle Informazioni

Un SGSI, Sistema di Gestione della sicurezza dei dati o *Information Security Management System*, consiste in un insieme di policies, procedure, linee guida, risorse ed attività associate raccolte collettivamente da una organizzazione, con il fine di proteggere i propri asset informativi [46].

Un SGSI rappresenta un approccio sistematico per stabilire ed attuare, succesivamente monitorare, operare, mantenere e migliorare la sicurezza delle informazioni di un'organizzazione, per proteggere e controllare le informazioni aziendali da modifiche volontarie o involontarie di dati o da accessi non autorizzati.

Non tutti i sistemi informativi diventano automaticamente SGSI; il sistema deve applicare le best practice indicate dagli standard ISO della famiglia 27000 - che nel caso in analisi è indicato in ISO 27001:2013 -, per poi ottenere una certificazione da un ente indipendente.

7.1 Ambito di Competenza e Controlli effettuati

Le informazioni meritevoli di tutela e protezione sono tutte quelle che possiedono valore in ambito aziendale in qualsiasi forma esse siano salvate [47] e quindi possono essere considerate tali anche i dati personali.

I controlli effettuati dal SGSI sui suddetti dati sono di aria natura:

- Deterrenti: ridurre al minimo le probabilità di attacchi volontari;
- Preventivi: proteggere le vulnerabilità, rendere inefficaci gli attacchi o ridurne l'impatto;
- Correttivi: ridurre gli effetti degli attacchi;
- Investigativi: scoprire gli attacchi e attivare controlli preventivi e correttivi.

In sintesi va ricordato che i controlli mirano non solo a proteggere le minacce, ma anche a ridurre le vulnerabilità, a limitare gli impatti di incidenti e a proteggere da qualunque rischio, sia interno che esterno.

7.2 Strutturazione

Un SGSI è un processo continuativo di ricerca, identificazione, definizione, risoluzione ed attuazione di misure a tutela dei rischi aziendali; si tratta quindi di un lungo processo a cascata, dove ogni passaggio necessita di essere concluso per poter passare a quello successivo.

Il ciclo deve essere mantenuto e aggiornato in considerazione della possibilità; è possibile che siano state create nuove minacce e vulnerabilità ed è richiesto quindi una nuova valutazione dei rischi aziendali. A questo punto sarà necessario ripercorrere il processo dal punto richiesto fino all'attuazione del SGSI, per attuare così tutte le misure necessarie per garantire il sistema. La stessa cosa può avvenire nel caso in cui vengano approvati nuovi standard, oppure quando sono richiesti ed attuati nuovi trattamenti ed attività di processamento delle informazioni.

Esistono due importanti processi all'interno del ciclo: valutazione del rischio e gestione del rischio.

Per quanto concerce alla valutazione del rischio, o *Risk assessment*, si individuano tutte quelle stime sulle minacce e sull'impatto delle stesse, sulle vulnerabilità delle informazioni e sugli impianti di elaborazione.

La gestione del rischio, o *Risk Management*, rappresenta tutti i processi di verifica, controllo, minimizzazione o eliminazione dei rischi inerenti la sicurezza che incidono sui sistemi elaborativi.

Definizione della politica per la sicurezza delle informazioni

Il processo è definito dai seguenti passi: in prima battuta è necessario definire obiettivi e perimetro di applicazione in termini di caratteristiche del business, organizzazione, logistica, tecnologia, beni, e così via. Successivamente si procede alla creazione della politica di sicurezza, valutando principi e obiettivi generali dell'azienda in ambito di sicurezza, oltre ai requisiti legali o aziendali; si procede poi alla definizione di una metodologia di valutazione del rischio, dove si indicano le soglie di accettazione.

Tutta questa parte è definita preparatoria; pur rientrando all'interno del ciclo di vita del SGSI essa rappresenta la definizione delle regole base per la gestione dei rischi. Combinando, infatti, interessi aziendali, regole normative di vari livelli, costi e benefici dei beni - informazioni o dati -, gestiti dal sistema stesso si produce una serie di policies; quest'ultime, combinate fra loro producono una politica, la politica per la sicurezza delle informazioni.

Definizione del perimetro del SGSI

Il prossimo passo riguarda la definizione del perimetro di azione del sistema di gestione; vanno in questo punto definiti i beni da tutelare, le minacce e vulnerabilità di competenza, e stime di impatto su possibili perdite di riservatezza, integrità, disponibilità che i beni possono ricevere.

Valutazione del Rischio

Successivamente si procede alla valutazione del rischio; il calcolo viene effettuato valutanto vari punti:

- danni derivati da violazione alla sicurezza;
- probabilità di possibili violazioni, analizzando minacce e vulnerabilità;
- stima del livello di rischio;
- valutazione del trattamento effettuato.

Si tratta di un passaggio molto complesso, in quanto stime sbagliate possono provocare danni, informazioni e dati compromessi, costi proibitivi. Infatti,

nel caso di stime non veritiere, l'investimento economico aziendale sarà effettuato sia per aumentare la protezione delle informazioni, sia per nel ripristinare situazioni precendenti ad attacchi. Per questo è essenziale produrre stime veritiere e il più fedeli possibili alla realtà aziendale.

Gestione del Rischio

A questo punto si procede alla gestione del rischio; vanno infatti identificati e stimati i trattamenti valutando i controlli. Non è sempre possibile fare fronte alla gestione dei dati all'interno dell'ambito aziendale; i costi troppo elevati, i rischi troppo alti possono portare al trasferimento presso enti esterni, a cui competono, a volte gli stessi trattamenti. Generalmente accade che la gestione del rischio sia di competenza aziendale: in questo caso è opportuno applicare i controlli stabiliti e accettare il rischio consapevolmente, in conformità sia alle polities aziendali, sia a quelle legate alla sicurezza delle informazioni.

Scelta dei Controlli

L'ultima parte di questa catena riguarda la definizione di tutte le azioni da compiere per l'attuazione e monitoraggio delle vulnerabilità e degli attacchi. Si tratta di definire metodologie, politiche, strumenti da utilizzare per verificare che l'attività proceda senza interruzioni, dove la sicurezza è verificata e dove i dati mantengano quelle caratteristiche tali da garantirne il valore e l'utilità aziendale.

E' previsto che ciascuna fase sia accompagnata da documentazione; non tutti i documenti indicati sono obbligatori, ma alcuni di essi sono richiesti non sono da aziende di certificazione, ma anche da organi controllori: Analisi dei Rischi correlati alla sicurezza, Manuali del SGSI sono solo alcuni esempi. Il più importante rimane la Dichiarazione di Applicabilità del SGSI: documento obbligatorio per ottenere la certificazione SGSI, esso contiene al suon interno la definizione di politiche, perimetro di azione, valutazione di rischi e gestione degli stessi.

7.3 Finalità

L'informazione rappresenta un bene contenente valore per l'organizzazione, dato che larga parte dei dati sono trattati, memorizzati, trasportati tramite supporti elettronici; quindi sulle stesse organizzazioni ricade il compito di garantire la sicurezza dei propri dati, in un contesto dove i rischi causati dalle violazioni dei sistemi informatici costituiscono il maggior pericolo.

Un SGSI ha come obiettivo [48]:

- assicurare la continuità dell'attività effettuata dall'organizzazione;
- minimizzare i danni derivanti da eventuali incidenti;
- massimizzare il rendimento del capitale investito e le opportunità di miglioramento.

Si evince dunque che la sicurezza delle informazioni rappresenta non solo una buona prassi atta a creare fiducia sul mercato e, successivamente, nei consumatori; essa rappresenta una responsabilità gestionale. Il *know how* aziendale, rappresentato da tutti i dati e le informazioni, deve essere tutelato, e deve essere fatto con priorità uguale in tutti i settori dell'attività.

E' per questo che gli organismi normatori hanno emanato diverse disposizioni in materia a cui vengono affiancati standard internazionazionali ISO; il fine ultimo di tutto ciò è quello di creare un modo organico, semplice ed efficace di trattazione del problema, riducendo da un lato l'impatto economico d'investimento.

Capitolo 8

Analisi dei rischi

Come indicato nel capitolo precedente, una parte fondamentale nello studio e nella creazione di un qualunque sistema, sia esso per il trattamento dei dati personali o per la gestione della sicurezza informatica, è analizzare i rischi.

Una corretta valutazione dei rischi permette il giusto investimento, sia in ambito economico che tecnologico, prevenendo minacce e vulnerabilità. Non deve essere, dunque, solo un obbligo legislativo, ma deve essere una buona prassi lavorativa, di progettazione, di sviluppo e di implementazione.

Sia il testo italiano in vigore [1], che quello europeo di futura approvazione [2], prevedono la definizione di un modello di trattamento dei dati basato su l'analisi dei rischi.

Si può leggere infatti:

> «*I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso*

[1] D.Lgs 30 giugno 2003, n.196 *Codice in materia di protezione dei dati personali*

[2] COM 2012/0011, *Proposta di regolamento del Parlamento Europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)*

non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta [3].»

ed ancora:

«*Previa valutazione dei rischi, il responsabile del trattamento e l'incaricato del trattamento prendono le misure [...] per proteggere i dati personali dalla distruzione accidentale o illegale o dalla perdita accidentale e per impedire qualsiasi forma illegittima di trattamento, in particolare la comunicazione, la divulgazione o l'accesso non autorizzati o la modifica dei dati personali* [4].»

8.1 Perdita o Distruzione di dati

Questo tipo di rischio è uno di quelli più frequenti non solo in contesto aziendale, ma anche in quello di tutti i giorni. Si tratta di perdere l'utilizzo, in maniera parziale o permanente, dei dati, contenuti in supporti di memorizzazione.

Sono tante le casistiche rientranti in questo ambito, e non tutte dipendono da errori di progettazione del sistema: basti considerare che molti degli attacchi informatici compiuti sfruttano tecniche di ingegneria sociale, scienza che studia il comportamento individuale al fine di carpire informazioni utili [49].

Questo tipo di tecnica frutta l'analisi di informazioni recuperate ad un soggetto scelto al fine di portare un attacco, di varia natura, per poter poi violare in maniera completa il sistema e carpire informazioni sempre più confidenziali.

E' una tecnica molto utilizzata in ambito aziendale dato che consente il reperimento di informazioni vitali per la stessa, portandola anche a rischio di fallimento. Sfruttando informazioni attendibili, come indirizzi mail interni alla stessa azienda o provenienti da servizi sicuri, i soggetti malintenzionati possono procedere a reperire informazioni dalle mail di risposta o dai file allegati aperti volontariamente dai mal capitati. Infatti questi ultimi non

[3] art. 31, D.Lgs n. 196/2003
[4] art. 30, COM 2012/11

sono altro che programmi di phishing, in grado di trasferire dati dall'azienda verso l'esterno.

Altre tecniche di attacco, chiamate *Denial of Service*, o DoS, possono provocare perdite momentanee di accesso ai dati; queste tecniche vanno a colpire le risorse di memorizzazione messe a disposizione dai server nel momento di accettazione di connessione. Colpendo, così, i computer contenenti le informazioni, è possibile rendere i dati indisponibili per un periodo limitato di tempo; è possibile che le strumentazioni possano subire danni e quindi non essere più utilizzate, ma non è il fine ultimo di questo genere di azioni.

Questi tipi di rischi, che derivano da azioni non compiute o fatte accidentalmente, necessitano di continuo studio, monitoraggio, controllo, dato che il progresso sia scentifico che tecnologico è in rapido aumento. Queste azioni sono quelle producenti più danni, dato che comportano furto, manomissione, compromissiome, distruzione del sistema.

Gli errori di progettazione possono portare a distruzione o perdita di dati: un sistema che non definisce correttamente gli accessi alle informazioni può permettere il compimento di azioni non ammissibili, non richieste, o impossibili per i criteri stabiliti, comportando a cancellazioni, parziali o totali, di informazioni utilizzate in ambito di trattamento.

Un profondo e completo studio delle dinamiche del sistema può permettere l'eliminazione di questa minaccia in maniera definitiva; verificato che se il sistema in questione implementa correttamente i meccanismi di autorizzazione ed autenticazione, non sarà necessario ricondurre ulteriori studi successivamente. Solo se si procede ad una modifica dei meccanismi sarà necessario riprocedere all'analisi per rilevare possibili falle nella gestione delle autorizzazioni.

8.2 Trattamento non Consentito o non Conforme

Per trattamento non consentito o non conforme si considera tutte quelle pratiche che non rispettano la normativa di rifermento in materia di trattamento dei dati.

Esempi in questo ambito potrebbero essere divulgazioni e comunicazioni non autorizzate dal Garante, - caso di trattamento non conforme -, o il pro-

cedimento al trattamento di talune informazioni su cui non sarebbe possibile, - caso di trattamenti non consentiti -. Se si effettuano operazioni di raccolta su particolari categorie di informazioni senza che si posseggano i giusti requisiti, - autorizzazioni, norme legislative, eccetera -, si ricade nell'ultima casistica.

In questo caso il rischio maggiore è legato alla diffusione di informazioni effettuata da soggetti interni all'ambito aziendale come titolari, responsabili o incaricati. L'estrazione non controllata di informazioni, o la visibilità di notizie non di propria competenza rappresenta una grave vulnerabilità, che naturalmente può essere arginata se viene attuato un controllo preciso e puntuale sul sistema prima che sia utilizzato. Non è possibile limitare la diffusione di informazioni da parte di soggetti che detengano tutti i requisiti per potervi accedere, ma è possibile definire dei codice deontologici per limitare al minimo il fenomeno.

Il trattamento non consentito rappresenta uno dei punti di più difficile controllo perchè l'unica azione attuabile per limitare il rischio consiste nel leggere attentamente la notifica presentata all'interessato e richiedere informazioni presso il Registro dei Trattamenti al Garante della Privacy.

8.3 Accesso non Autorizzato

L'accesso non autorizzato rappresenta uno dei rischi più forti in ambito aziendale; chiunque riesca ad entrare nel sistema, pur non possedendone i requisiti per farlo, rappresenta un pericolo. Questo stesso soggetto potrebbe compiere azioni a lui non consentite, compromettendo il sistema, i dati contenuti nel sistema e la sicurezza degli interessati.

Controlli accurati e misure di protezione sono richieste per ridurre questo rischio; come vale per i casi di distruzione e perdita, è importante mantenere un livello di analisi e ricerca costante ma preciso, per limitare queste vulnerabilità sia in ambito interno, che in ambito esterno.

8.4 Criticità nei dati

Qualunque compromissione di dati rappresenta un rischio in ambito aziendale, soprattutto in materia di trattamento; infatti verrebbe a mancare uno dei principi fondamentali, la tutela della privacy,

I rischi legati ai dati riguardano la compromissione delle caratteristiche a loro attribuiti, ovvero integrità, riservatezza, disponibilità, autenticità.

Esistono due ambiti di analisi: quello interno del sistema e quello esterno. In ambito interno la compromissione dei dati può avvenire per diverse cause; errori umani, cattiva gestione.

Utenti non consapevoli possono produrre azioni compromettenti per il sistema stesso, portando ad esempio, ad avere copie di dati diverse; questo comporta la perdita di integrità dei dati, dato che non è più possibile risalire a quelli originali e veritieri. Possibili cancellazioni di parti di informazioni dal sistema centrale riducono la disponibilità dei dati, dato che talune notizie non saranno più recuperabili. La divulgazione di notizie poi, come avviene nel caso di trattamenti non conformi, comportano la perdita di riservatezza.

Gli errori di cattiva programmazione sono riconducibili alla non corretta applicazione di norme basilari legate alla sicurezza dei dati; i principi precedentemente indicati rappresentano il punto cardine nella costituzione di sistemi sicuri. Se non esistono meccanismi tali da impedire accessi ai sistemi da utenti non autorizzati, se non esistono copie di sicurezza delle stesse informazioni in maniera tale da ricostruire a ritroso la veridicità e l'integrità del sistema, allora non è possibile creare un luogo dove i rischi sono ridotti al minimo.

L'ambito esterno è dominato da tutte quelle azioni atte a compromettere i dati interni; attacchi di varia natura possono provocare gravi danni, non solo per perdita di disponibilità dei dati, bensì per perdita di riservatezza e di integrità. Questo tipo di rischi, come indicato precedentemente richiede uno studio costante e completo, in modo da garantire una rapido ed efficente azione di difesa.

Capitolo 9

Cotromisure preventive e reattive

Analizzato il contesto lavorativo, tramite i SGSI, e i rischi che si possono riscontrare in questo ambito, tramite il capitolo precedente, questo capitolo si occuperà delle contromisure da atturare. Si procederà con un'analisi a più livelli, considerando sia gli obblighi legislativi, sia le misure introdotte da PETs e PbD.

9.1 Misure Minime ed Idonee di Sicurezza

Il D.Lgs n.196/2003 contiene al suo interno una serie di articoli, dal 33 al 36, recante una serie di misure obbligatoriamente attuabili da parte dei titolari di trattamento a tutela degli stessi e degli interessati.

Si fa riferimento in questo contesto a due diversi tipi di misure; quelle minime e quelle idonee. La differenza sostanziale fra le due categorie è rintracciabile nelle attribuzioni legali in caso di processo: il non rispetto delle misure minime di sicurezza comporta il profilare di un reato penale, mentre nel caso delle misure idonee si profila la violazione di un atto amministrativo, sanzionato in maniera meno grave.

L'applicazione dunque di entrambe gli atti rappresenta un passo importante non solo per tutelare l'azienda rispetto a possibili rischi interni ed esterni, ma per garantire fiducia ai possibili clienti e quindi al mercato.

Le misure minime sono indicate nell'articolo 34, che esplicitamente prevede l'uso di:

- autenticazione informatica;
- adozione di procedure di gestione delle credenziali di autenticazione;
- utilizzazione di un sistema di autorizzazione;
- aggiornamento periodico rivolto ad incaricati, addetti alla gestione o manutenzione della strumentazione tecnologica;
- Protezione delle strumentazioni tecnologiche e dei dati rispetto a trattamenti illeciti, accessi non consentiti, determinati programmi informatici;
- adozione di procedure per la creazione e custodia di copie di sicurezza, ripristino della disponibilità dei dati e dei sistemi;
- adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare particolari informazioni, quali la salute o la vita sessuale.

Si tratta di principi base di sicurezza, centrati sul mantenimento della continuità lavorativa e volti ad eliminare le criticità legate ai dati. Meccanismi di autenticazione ed autorizzazione garantiscono la riservatezza delle informazioni, mentre sistemi di creazione di copie di sicurezza permetteno di garantire integrità e disponibilità dei dati.

L'allegato B dello stesso codice indica in maniera più esplicita l'applicazione di talune misure minime, definendo tecnologie e metodologie di utilizzo e configurazione delle stesse. Larga parte è dedicata alle specifiche riguardanti l'autenticazione informatica e all'autorizzazione, descrivendo in maniera esplicita linee guida e profili di utilizzazione; nel caso di autenticazione informatica è importante ricordare l'autenticazione riconosciuta tramite possibili strumenti, - token, strumenti biometrici -, e la definizione di profili diversi di autenticazione concessi allo stesso utente per il compimento di diverse mansioni.

E' indicata esplicitamente la necessità, da parte del titolare o del responsabile del trattamento, di definire disposizioni scritte atte a garantire il proseguimento dell'attività nel momento in cui soggetti con credenziali di accesso risultino assenti per prolungati periodi di tempo.

Nel testo si esplicano, poi, tutte le regole da ottemperare nel caso di utilizzo di strumentazioni esterne per provvedere alla applicazione di misure di sicurezza minimi, oltre alla indicazione dei periodi temporali per prevedere copie di sicurezza, corsi di aggiornamento e documenti di attribuzioni di responsabilità lavorative.

9.2 Misure Consolidate PETs

I principi PETs hanno origini più lontane rispetto alla normativa sopra citata, ma non per questo datate; è vero che queste tecnologie hanno dei difetti, soprattutto a livello implementativo, ma i principi rimangono ancora validi, come indicato nel capitolo 2.

Tecnologie di cifratura, metodologie di anonimizzazione e sistemi di filtrazione delle informazioni sono strumenti tuttora validi per limitare vulnerabilità e possibili danni. Assieme a questi vanno ricordati antivirus e firewall per limitare attacchi esterni e eliminare possibili distruzioni e perdite; protocolli di autenticazione-autorizzazione-accounting garantiscono trattamenti pertinenti alle norme e alle finalità di raccolta, non intaccando le caratteristiche legate ai dati. Da ricordare infine misure per determinare il perimetrazione del perimetro e gestione degli accessi.

9.3 Misure Emergenti PbD

Le misure Privacy By Design sono di più recente approvazione ma mantengono ancora valide le contromisure PETs sopra indicate. Largo spazio viene dedicato alla difesa della privacy e, di conseguenza, alla tutela degli utenti; tecniche di data mining, di de-identificazione sono solo alcuni esempi in questo senso.

Da ricordare poi tutte quelle misure attee a garantire il rispetto del concetto di privacy in tutto il ciclo di vita del trattamento; misure per la com-

pleta e totale distruzione dei dati, come previsto per legge, piattaforme che trattengano i dati personali come HIDE, strumenti di sicurezza che siano più garantisti possibili.

9.4 Tabella Comparativa PETs e PbD

Si propone una tabella riassuntiva e comparativa; per ciascun punto di analisi considerato verranno indicati i punti di criticità, o ambito di rischio, e le contro misure sia provenienti da PETs che da PbD.

Ambito di Rischio			Contromisure		
			Privacy Enhancing Tecnologies	Privacy by Design	
Dati ed Informazioni		Dati e Informazioni Documenti			
Documenti	**Riservatezza**	Violazione Acquisizione di informazioni non rilasciate	Crittografia reversibile: cifratura simmetrica; asimmetrica. Steganografia; Anonymity and Obfuscation Data.	Data Mining Analytical Tecnologies; Data Correlation.	Semantic Web Suite XML: XML Signature; XML Encription; Identity XML; Identity Web Services. Sistemi di non repudiabilità: es. PEC
	Integrità	Alterazione Rispetto alla fonte dei dati originali	Crittografia irreversibile: Funzioni Hash. Tecniche di Watermarking (Media).	Public Key Infrastructure.	
	Autenticità	Alterazione rispetto all'autore originale	Crittografia reversibile: Firma digitale; Certificati digitali (X.509, PGP). Tecniche di Watermarking (Media).	Intellectual Property Rights Management.	Identity and Attributes Management System; Profile Management System.
	Disponibilità	Negazione di accesso ed acquisizione dei dati	Disaster Recovery; Services Continuity; Back-up; Copie di sicurezza.	Business Continuity Plan; Trasparency Tools; Reliability, Robusteness and Abuse Prevention Tool.	

Ambito di Rischio			Contromisure	
			Privacy Enhancing Tecnologies	**Privacy By Design**
			Sistemi e Trattamento	
Reti e Web Application	**Intrusioni**	Accesso non consentito, Negazione di servizio.	Sistemi di Perimetrazione Rete; Firewall di Rete; Analisi e Log Tracking; Network Intrusion Detection System; Virtual Private Network.	Network Monitoring Diagnostic Tool.
	Attacchi			
Sistemi Applicativi	**Sicurezza**	Accesso non consentito. Negazione od alterazione di servizio.	Antivirus; Antimalware; AntiSpyware; Personal Firewall.	Monitoring Diagnostic Tool; Reliability, Robustness, Abuse Prevention Tools.
	Affidabilità		Intrusion Detection System; Disaster Recovery; Protocolli di riservatezza ed autenticità: SSL v3, S-MIME.	
Trattamento	**Distruzione**	Perdita ed utilizzo illecito dei dati, Perdita del controllo sulle informazioni.	Back-up; Copie di Sicurezza; Analisi e Log Tracking.	Business Continuity Plan; Minimizzazione dei Dati; Trasparency Tools; Reliability, Robustness, Abuse Prevention Tools.
	Perdita			
	Non Consentito			
	Non Conforme			
Utenti	**Accesso**	Rilascio di accesso e permessi non associati al soggetto.	Analisi e Log Tracking; Protocolli A.A.A.: Autentication, Authorization, Accounting basati su ruoli, e credenziali a vari livelli: password, token, certificati digitali, smartcard, tecniche biometriche.	Identity and Attributes Management Systems; Profile Management Systems; Accountability Management Systems; Access Control Management System; Privacy Policies Management System.
	Autenticazione			
	Autorizzazione			

Parte IV

Conclusioni

Capitolo 10

Conclusioni

L'obiettivo inziale della Tesi è stato quello descrivere il concetto di privacy e le relative minacce e contromisure con riferimento ai contesti di gestione (aziendale e Big Data) e al quadro normativo vigente. Con riferimento alle contromisure l'elaborato ha illustrato quelle tradizionali, note come Privacy Enhanced Technologies (PETs) e quelle emergenti note come Privacy by Design (PbD).

Con riferimento a queste ultime si sono illustrate in dettaglio i principi e le prassi PbD e la figura del Privacy Officer formalmente riconosciuta dal novellato giuridico.

L'obiettivo della tesi è stato quindi quello di analizzare su base comparativa i due approcci in modo da meglio comprendere la portata innovativa del PbD.

Fatte queste premesse, rispetto agli obiettivi illustrati in introduzione il risultato conseguito può essere così sintetizzato.

Il Privacy by Design (PbD) è stato introdotto per risolvere limitazioni e criticità delle tecnologie Privacy Enhanced Technologies (PETs).

Tali criticità sono riconducibili alla natura "add-on" e non "embedded" delle contromisure PETs a protezione delle informazioni personali archiviate o trasmesse in rete. Ciò ha determinato due principali fattori:

1. Le PETs non hanno garantito - complice l'evoluzione della comunicazione in rete verso uno scenario di Big Data esponenzialmente alimentato da Web Application e Social Media - il mantenimento nel tempo

del controllo da parte dell'utente delle proprie informazioni personali e non;

2. La natura "add-on" ha, in taluni casi, modificato le modalità di fruizione di un servizio rispetto alle caratteristiche originali dello stesso, compromettendo spesso trasparenza e soprattutto facilità di utilizzo da parte dell'utente che ha, quindi, percepito i componenti aggiuntivi di sicurezza come qualcosa "difficile" o "poco chiaro", se non al limite ostacolante. Ciò in definitiva ha impattato negativamente sulla fiducia e sull'efficace utilizzo delle PETs. Pensiamo per esempio alla posta elettronica e al marginale utilizzo dei componenti S-Mime che doterebbero un normale scambio di messaggi di riservatezza, integrità e autenticità.

La fattiva portata applicatica del PbD è ancora in fase di affermazione, benchè tale metodologia sia sta "accreditata" a livello normativo con la proposta di regolamento Europeo 2012/2011 sulla protezione dei dati personali e la libera circolazione degli stessi.

Nel presupposto consolidato che il PbD è un insieme di prassi e di metodologie esplicate in 7 principi fondamentali, piuttosto che vere e proprie tecnologie, il valore aggiunto fornito è quello di proporre un framework di progettazione che inserisca il requisito di protezione delle informazioni fin dalla pianificazione del sistema informativo che gestirà tali informazioni e rispetto al quale la centralità dell'utente (o soggetto interessato) e il ruolo di chi gestirà tale sistema sono poste sullo stesso piano della tecnologia utilizzata.

Tale proposta del Parlamento e del Consiglio d'Europa prevede esplicitamente un nuovo attore "responsabile per la protezione dei dati personali" o Privacy Officer (PO) le cui competenze devono essere di carattere multidisciplinare comprendendo sia quelle di carattere gestionale, che giuridico, che tecnico.

In linea ai principi del PbD la principale responsabilità del PO - il quale deve avere una completa e approfondita consapevolezza dei rischi e delle vulnerabilità che minacciano un sistema informativo - sarà quella di prevenire e non quella di riparare al fine di concorrere a garantire che un sistema

di gestione delle informazioni (laddove per gestione si intende principalmente trattamento e processamento delle informazioni) si mantenga nel tempo sicuro e affidabile.

L'esito dell'elaborato, in un contesto in cui la fattiva portata applicativa del PbD è ancora in fase di definizione, si concretizza nel rappresentare tramite una tabella comparativa i due diversi approcci (PbD e PETs) e come questi implementino le contromisure rispetto ai principali ambiti di rischio.

La tabella rappresenta una ricognizione delle principali contromisure rispetto alle vulnerabilità su informazioni e sistemi informativi.

Dalla tabella si può rilevare che il PbD non sostituisce le PETs ma se ne avvale e anche in maniera sostanziale completandole laddove queste nel corso della loro applicazione hanno presentato limitazioni o criticità. Il completamento, allo stato ed è verosimile che lo sarà anche in prospettiva, è attuato su base gestionale introducendo regole e politiche di gestione rispetto alle quali si rivela centrale sia il ruolo dell'utente sia del Privacy Officer.

Eventuali sviluppi futuri della Tesi potrebbero riguardare l'implementazione, rispetto ad uno dei 7 principi del PbD, di una specifica contromisura indicata nella tabella: ad esempio quello di maggiore caratteristica applicativa attinente la centralità dell'utente. (User-Centric).

Bibliografia

[1] ZAPPA, FLAVIA (2015) - La Criminalità Informatica e i Rischi per l'Economia e le Imprese a Livello Italiano ed Europeo. [PDF] Disponibile a: <http://www.unicri.it/in_focus/files/Presentazione_Lucca_2.pdf>. [Ultimo accesso: 5 marzo 2015].

[2] WIKIPEDIA (2014) - Social Network. [online] Disponibile a: <http://en.wikipedia.org/wiki/Social_network>. [Ultimo accesso: 10 novembre 2014].

[3] PETTEY, CHRISTY; GOASDUFF, LAURENCE (2011) - Gartner Says Solving 'Big Data' Challenge Involves More Than Just Managing Volumes of Data. [online] Disponibile a: <http://www.gartner.com/newsroom/id/1731916>. [Ultimo accesso: 12 novembre 2014].

[4] TELECOMITALIA (2014) - Big Data & privacy - Video intervista. [online] Disponibile a: <http://www.telecomitalia.com/tit/it/bigdatachallenge/interview-clippinger.htm l>. [Ultimo accesso: 12 novembre 2014].

[5] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (2006) - Linee guida sul trattamento di dati personali dei lavoratori privati. [online] Disponibile a: <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1364 939>. [Ultimo accesso: 14 novembre 2014].

[6] PALMIRANI, MONICA; MARTONI, MICHELE (2012) - *Informatica Giuridica per le Relazioni Aziendali*. G. Giappichelli Editore.

[7] POLACCACCHINI, MARCELLO (2009) - *Privacy in Azienda*. Capitolo 1. IPSOA Editore.

[8] VAN BLARKOM, G.W.; BORKING, J.J.; OLK, J.G.E. (2003) - *Handbook of Privacy and Privacy-Enhancing Technologies*. College Bescherming Persoonsgegevens. [PDF] Disponibile a: <http://www.andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf>. [Ultimo accesso: 17 novembre 2014].

[9] WIKIPEDIA (2014) - Anonimyzer. [Online] Disponibile a: <http://en.wikipedia.org/wiki/Anonymizer> [Ultimo accesso: 10 dicembre 2014].

[10] CAVOUKIAN, ANN (2009) - Moving Forward From PETs to PETs Plus: The Time for Change is Now. [PDF] Disponibile a: <http://www.privacybydesign.ca/content/uploads/2009/01/petsplus.pdf>. [Ultimo accesso: 17 novembre 2014]

[11] LANGHEINRICH, MARC - Privacy By Design - Principles of Privacy-Aware Ubiquitous Systems. [PDF] Disponibile a: <http://cs.gmu.edu/jpsousa/classes/699/papers/privacyLangheinrich.pdf> [Ultimo accesso 10 dicembre 2014]

[12] Registratiekamer, The Netherlands (1995) - Privacy-Enhancing Technologies: The Path to Anonymity Vol.2. [PDF] Disponibile a: <http://www.privacybydesign.ca/content/uploads/1995/03/anoni-v2.pdf>. [Ultimo accesso: 10 dicembre 2014].

[13] WIKIPEDIA (2014) - Anonimyzer. [Online] Disponibile a: <http://en.wikipedia.org/wiki/Anonymizer> [Ultimo accesso: 10 dicembre 2014].

[14] VELLANKI, B. (2003) - Privacy Enhancing Technologies (PET). [PPT] Dosponibile a: <https://www.cs.purdue.edu/homes/bb/hel3.ppt>. [Ultimo accesso: 17 novembre 2014].

[15] AAVV - Incogno Corporation Launches Incogno SafeZone(TM), The First Merchant Solution for Anonymous E-Commerce. [Online] Disponibile a: <http://www.prnewswire.com/news-releases/incogno-corporation-launches-incogno-sa fezonetm-the-first-merchant-solution-for-anonymous-e-commerce-73322057.html>. [Ultimo accesso: 10 dicembre 2014].

[16] W3C - Platform for Privacy Preferences (P3P) Project. [Online] Disponibile a: <http://www.w3.org/P3P/>. [Ultimo accesso: 18 novembre 2014].

[17] SULLIVAN, D. (2012) - Google: "Impractical" To Comply With IE's P3P Privacy Controls; Microsoft, Facebook and Others Also Fail. [Online] Disponibile a: <http://marketingland.com/google-impractical-to-comply-with-ie-privacy-6543>. [Ultimo accesso: 18 novembre 2014].

[18] META groups (2008) - Privacy Enhancing Tecnologies, Report v.1.1. [Online] Disponibile a:<https://danskprivacynet.files.wordpress.com/2008/07/rapportvedrprivacyenhancingtechlologies.pdf>. [Ultimo accesso: 18 novembre 2014].

[19] CAVOUKIAN, ANN (2012) - Privacy by Design: Origins, Meanings and Prospects for Assuring Privacy and Trust in the Information Era. In: YEE, G.O.M. (ed.), *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards*, pp. 170-208. Information Science Reference.

[20] WIKIPEDIA (2011) - Fair Information Practice. [online] Disponibile a: <http://en.wikipedia.org/wiki/FTC_Fair_Information_Practice>. [Ultimo accesso: 26 novembre 2014].

[21] IT LAW WIKI (2013) - Fair Information Practise Principles. [online] Disponibile a: <http://itlaw.wikia.com/wiki/Fair_Information_Practice_Principles>. [Ultimo accesso 27 novembre 2014].

[22] CARE, FRED H. (2006) - The Failure of Fair Information Practice Principles. In: WINN, JANE K. (Ed.), *Consumer Protection in the Age of the 'Information Economy'*, pp. 341-378. Ashgate Publishing Company.

[23] OHLDEN, ANNA (2004) - Landmark Resolution Passed To Preserve The Future Of Privacy. [online] Disponibile a: <http://www.science20.com/newswire/landmark_resolution_passed_preserve_future_privacy>. [Ultimo accesso 28 novembre 2014].

[24] CAVOUKIAN, ANN (2014) - Privacy by Design: I 7 principi fondazionali. [PDF] Disponibile a: <http://www.privacybydesign.ca/content/uploads/2012/04/7foundationalprinciples-italian.pdf>. [Ultimo accesso 28 novembre 2014].

[25] WIKIPEDIA (2014) - Legge sulla privacy. [online] Disponibile a: <http://it.wikipedia.org/wiki/Legge_sulla_privacy>. [Ultimo accesso 4 dicembre 2014].

[26] MINISTERO DELL'INTERNO (2014) - Gli Accordi di Schengen. [online] Disponibile a: <http://www.interno.gov.it/mininterno/export/sites/default/it/sezioni/sala_st ampa/speciali/cittadini_europa/scheda_18519.html> [Ultimo accesso 4 dicembre 2014].

[27] COM(2010)609 def. del 4 novembre 2010, *Un approccio globale alla protezione dei dati personali nell'unione europea*

[28] COM(2012)11 def. del 25 gennaio 2012, *Proposta di regolamento del Parlamento Europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati.*

[29] CAVOUKIAN, ANN (2012) - Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices. [Online] Disponibile a: <http://www.privacybydesign.ca/content/uploads/2013/01/operationalizing-pbd-guid e.pdf>. [Ultimo accesso: 30 dicembre 2014].

[30] WIKIPEDIA (2014) - Piwik. [online] Disponibile a: <http://it.wikipedia.org/wiki/Piwik>. [Ultimo accesso: 15 febbraio 2015].

[31] PIWIK (2009) - Piwik. [online] Disponibile a: <http://piwik.org/>. [Ultimo accesso: 15 febbraio 2015].

[32] PIWIK (2008) - History. [online] Disponibile a: <http://piwik.org/history/>. [Ultimo accesso: 15 febbraio 2015]

[33] PIWIK (2008) - What is Piwik?. [online] Disponibile a: <http://piwik.org/what-is-piwik/> [Ultimo accesso: 15 febbraio 2015]

[34] PIWIK (2008) - Privacy. [online] Disponibile a: <http://piwik.org/privacy/>. [Ultimo accesso: 15 febbraio 2015]

[35] WIKIPEDIA (2015) - Do Not Track. [online] Disponibile a: <http://en.wikipedia.org/wiki/Do_Not_Track>. [Ultimo accesso: 15 febbraio 2015].

[36] OpenPDS(2012) - OpenPDS. [online] Disponibile a: <http://openpds.media.mit.edu>. [Ultimo accesso: 22 febbraio 2015].

[37] DE MONTJOYE, YVES-ALEXANDRE; SHMUELI, EREZ; WANG, SAMUEL S.; PENTLAND, ALEX SANDY (2014) - openPDS: Protecting the Privacy of Metadata through SafeAnswers. [online] Disponibile a: <http://www.plosone.org/article/fetchObject.action?uri=info:doi/10.1371/journal.pone.0098790&representation=PDF>. [Ultimo accesso: 20 febbraio 2015].

[38] GARDNER, JAMES (2010) - hide-emory. [online] Disponibile a: <https://code.google.com/p/hide-emory/wiki/Overview>. [Ultimo accesso: 20 febbraio 2015].

[39] WIKIPEDIA (2015) - Health Insurance Portability and Accountability Act. [online] Disponibile a: <http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act>. [Ultimo accesso: 20 febbraio 2015].

[40] GARDNER, JAMES; XIONG, LI (2008) - HIDE: An Integrated System for Health Information DE-identification. [online] Disponibile a: <http://www.mathcs.emory.edu/lxiong/research/pub/xiong08hide.pdf>. [Ultimo accesso: 20 febbraio 2015].

[41] SWEENEY, LATANYA (2015) - Bio. [online] Disponibile a: <http://dataprivacylab.org/people/sweeney/bio.html>. [Ultimo accesso: 20 febbraio 2015].

[42] WIKIPEDIA (2015), Named-entity recognition. [online] Disponibile a: <http://en.wikipedia.org/wiki/Named-entity_recognition>. [Ultimo accesso: 20 febbraio 2015].

[43] WIKIPEDIA (2014) - Datenschutzbeauftragter. [online] Disponibile a: <http://de.wikipedia.org/wiki/Datenschutzbeauftragter>. [Ultimo accesso: 22 dicembre 2014].

[44] WIKIPEDIA (2014) - Bundesdatenschutzgesetz. [online] Disponibile a: <http://de.wikipedia.org/wiki/Bundesdatenschutzgesetz> [Ultimo accesso: 22 dicembre 2014].

[45] DI BERNARDI, NICOLA; PEREGO, MONICA, POLACCHINI MARCELLO, SOFFIENTINI MARCO (2013) - Privacy Officer. IPSOA Editore, Milano, 400 pp.

[46] INTERNATIONAL STANDARD (2014) - Information tecnology - Security techniques - Information security management system - Overview and vocabulary. [online] Disponibile a: <http://standards.iso.org/ittf/PubliclyAvailableStandards/c063411_ISO_IEC_27000_2014.zip>. [Ultimo accesso: 24 febbraio 2015].

[47] STS CONSULTING (2006) - Sistemi di Gestione per la Sicurezza delle Informazioni. [online] Disponibile a: <http://torlone.dia.uniroma3.it/sistelab/sts.pdf>. [Ultimo accesso: 24 febbraio 2015].

[48] UNINFORM (2015) - I Sistemi di Gestione della Sicurezza dei Dati (SGSI - ISMS) ISO 27001/ISO 17799. [PDF] Disponibile a: <http://uninform.com/pdf/pdf_news/sis_gest_sicurezza.pdf>. [Ultimo accesso: 24 febbraio 2015].

[49] WIKIPEDIA (2015) - Ingegneria Sociale. [Online] Disponibile a: <http://it.wikipedia.org/wiki/Ingegneria_sociale>. [Ultimo accesso: 28 febbraio 2015]

Ringraziamenti

Un sincero e grande ringraziamento alla mia famiglia per il sostegno che mi ha dato in tutti questi anni; grazie a loro sono arrivata fin qui, è l'ho fatto al meglio delle mie possibilità.

Un ringraziamento forte va alla Dot.sa Prestipino e alla Prof.sa Brighi: la loro pazienza e il loro immenso aiuto hanno permesso la comprensione di questione giuridiche; inoltre la lor pazienza nei miei riguardi hanno portato alla stesura di questo elaborato.

Infine vorrei ricordare tutti i professori che hanno sostenuto i corsi universitari: grazie alla loro passione e alla loro dedizione hanno instaurato quella passione nell'insegnamento materie tale da far approfondire ogni singolo ambito, anche se le valutazioni non lo costatavano.