Dalla protezione dei dati personali come "sovrastruttura" dei processi di trattamento alla protezione fin dalla progettazione.
Il principio della "privacy by design" nel Regolamento UE 2016/679

Abstract

Si sente nominare la privacy by design ormai da qualche anno, almeno dall'entrata in vigore del Regolamento UE 679/2016.
Ma che cos'è, o meglio, cosa si intende quando ci si riferisce al termine Privacy by design?

Il concetto di privacy si è evoluto e continuerà ad evolversi di pari passo con i mutamenti della società[1], influenzata, oggigiorno, soprattutto dall'evoluzione tecnologica.
Si è passati dal right to be let alone (diritto di essere lasciati soli) come pressoché unico modo di concepire la privacy - che beninteso non è scomparso ma è una delle tante sfaccettature della privacy stessa[2] – alla sua evoluzione come dritto di mantenere il controllo sui dati personali oggetto di trattamento da parte di terzi.

L'avanzare della tecnologica, che spinge verso una società sempre più digitalizzata, sta determinando, o meglio sta facendo emergere come predominante, la problematica legata alla "gestione" del fenomeno del trattamento dei dati personali, in cui non si pongono tanto problemi nuovi – o almeno non necessariamente - quanto la necessità che questi vengano affrontati con strumenti o approcci diversi.
Prendendo in prestito le parole di **D.J. Solove** si può affermare che: "*La concezione della privacy deve rispondere alla realtà sociale, poiché la privacy è un aspetto delle pratiche sociali […] tuttavia la privacy non è neanche una questione solamente empirica; se ci concentrassimo semplicemente sulle attuali aspettative di privacy della gente, la nostra concezione di privacy si ridurrebbe continuamente data la crescente sorveglianza nel mondo moderno. Allora la privacy è anche una questione di potere, il prodotto di una visione della struttura sociale più ampia*".[3]

Il cambiamento della società tutta sta ridefinendo i confini di ciò che è possibile e non è possibile fare con i dati personali di altri soggetti, tanto che si è arrivati a un livello tale di "pervasività" nella sfera personale altrui - e le basi giuridiche di cui all'art. 6 GDPR, non più incentrate in maniera predominante sul consenso, stanno lì a dimostrarlo – che anche il diritto ha dovuto adeguarsi, e lo ha fatto, o almeno cerca di farlo in un modo molto intelligente, portandolo ad operare allo stesso livello della tecnica, cioè concependo il diritto stesso non tanto e non solo come "mero principio" da tenere in considerazione al momento di implementare il trattamento, o come **tutela successiva** nei confronti di un trattamento illecito di dati personali, ma come **presupposto stesso della tutela.**
Il diritto cioè, è portato ad operare ex ante, by design, laddove si progetta come verrà trattato il dato.
O per lo meno questo dovrebbe essere il senso dell'art. 25 GDPR: "Protezione dei dati (personali) fin dalla progettazione e protezione per impostazione predefinita".

Sommario

---

[1] https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2086&context=faculty_publications pag. 1141
[2] https://www.agendadigitale.eu/sicurezza/privacy/privacy-e-protezione-dati-personali-cosa-sono-quali-differenze-cosa-e-cambiato-col-gdpr/ (in questo contributo il termine Privacy – esclusivamente per motivi legati alla fluidità del testo - sarà considerato come sinonimo di protezione dei dati personali)
[3] https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2086&context=faculty_publications pag. 1142

1. Privacy by design, brevi cenni storici

1.1. Dalle FIPPs alle PETs al parere del GEPD sulle tecnologie ICT

Il dibattito intorno alla privacy e in particolare agli strumenti per implementarne la sicurezza e tutelarne la riservatezza è risalente; varie infatti sono state negli anni le iniziative volte a migliorare la privacy dei cittadini, sono stati pensati e predisposti accorgimenti con il preciso scopo di limitare i dati oggetto di trattamento e preservare la riservatezza stessa dei soggetti interessati.
Tra questi accorgimenti si possono sicuramente annoverare le "**FIPPs**"[4] (**Fair information practices Principles**) che costituiscono un insieme di indicazioni/pratiche – elaborate dalla Federal Trade Commission degli USA e condivisi anche a livello internazionale dall'OCSE – in materia di privacy, e le "**PETs**"[5] (**Privacy Enhancing Technologies**), quei prodotti e quelle tecnologie progettate allo scopo di **rafforzare** e **migliorare** la protezione della privacy.

Tuttavia, le crescenti preoccupazioni, soprattutto nella prima decade del nuovo millennio in cui forte si è sentita la spinta delle nuove tecnologie[6], in particolare nell'ambito **ICT**, - tanto che si parla ormai di "**ubiquitous computer**"[7] a sottolineare l'onnipresenza del computer e di internet in ogni ambito della vita umana - hanno condotto le istituzioni europee a prendere in seria considerazione l'idea che, dando per pacifico che fermare la tecnologia non sarebbe stato ne possibile ne tantomeno auspicabile, l'unico modo per garantire la vita privata dei cittadini dalle crescenti invasività della tecnologia fosse quella di pensare ad un approccio nuovo e del tutto diverso alla privacy, volto a **generare fiducia negli individui**.
In questo senso si è espresso anche il **GEPD** (Garante europeo della protezione dei dati), in un suo parere del 2010[8]:
"*I potenziali benefici delle TIC (tecnologie dell'informazione e della comunicazione) possono essere sfruttati in pratica soltanto se sono in grado di generare fiducia, in altri termini, se possono assicurare la disponibilità degli utenti a dipendere dalle TIC a causa delle loro caratteristiche e vantaggi. Tale fiducia si produrrà soltanto se le TIC saranno affidabili, sicure, sotto il controllo degli individui e se verrà garantita la protezione dei dati e della vita privata* […]. *Tuttavia la soluzione a questi rischi per la vita privata e la protezione dei dati non può essere di eliminare, escludere o rifiutare di utilizzare o promuovere le TIC. Ciò non sarebbe né fattibile né realistico, impedirebbe agli individui di godere dei benefici delle TIC e limiterebbe seriamente i vantaggi generali da ottenere. […] Il GEPD ritiene che una soluzione più positiva consista nel progettare e sviluppare le TIC in modo da rispettare la vita privata e la protezione dei dati. È quindi fondamentale che la vita privata e la protezione dei dati siano incluse all'interno dell'intero ciclo di vita della tecnologia, dalla primissima fase di progettazione fino alla loro ultima distribuzione, all'utilizzo e all'eliminazione finale. Ciò viene indicato generalmente come principio della «privacy by design»".*

[4] https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/

[5] http://www.amblav.it/Download/MEMO-07-159.pdf
[6] https://www.ilprimatonazionale.it/scienza-e-tecnologia/tecnologia-2000-2020-gli-anni-del-boom-di-internet-160174/
[7] https://en.wikipedia.org/wiki/Ubiquitous_computing
[8] https://edps.europa.eu/sites/edp/files/publication/10-03-19_trust_information_society_it.pdf

2. Ann Cavoukian, la madre della Privacy by design

Lo studio di questo approccio "nuovo" alla privacy, quello che appunto viene chiamato "privacy by design" (nel prosieguo del testo anche **PbD**), non è altrettanto nuovo nel panorama dottrinale.
Fu infatti **Ann Cavoukian**[9] verso la fine del secolo scorso a coniare e riflettere su questo concetto.
Nell'ottica dell'autrice PbD realizzava la tutela della riservatezza dei dati personali sin dal principio, cioè sin dalla progettazione del trattamento, in modo tale da approcciarsi alla privacy non tanto e non solo tenendo conto delle leggi di settore, ma concependo il trattamento stesso come una fusione di tecniche e normativa di settore a creare un "procedimento" che contenesse già in se le basi per un trattamento sicuro del dato.
In questo modo veniva anticipata la tutela, che non doveva attendere tanto la violazione del dato per poi far scattare la retribuzione sottoforma di sanzione, ma poneva le basi affinché questa violazione non si verificasse.

L'approccio dell'autrice è proattivo piuttosto che difensivo ma, beninteso, essa non considera affatto la pbd come mero strumento atto a conferire conformità rispetto ad una regola giuridica, lo inquadra piuttosto come strumento positivo a disposizione di strutture pubbliche e private che proprio dall'implementazione di tale concetto potrebbero trarre vantaggio in termini di riduzione di costi, innovazione tecnologica, competitività, nonché di efficacia ed efficienza nell'azione amministrativa.
In altre parole è proprio l'implementazione di tale concetto che tende a costruire quel legame di fiducia tra il titolare del trattamento e i soggetti interessati.[10]

2.1. Resolution of Jerusalem

Pietra miliare nel dibattito intorno al tema della privacy by design fu la "Resolution of Jerusalem"[11], 32° conferenza internazionale dei Garanti della privacy[12] tenutasi a Gerusalemme nel 2010[13].
Nella stessa fu riconosciuta l'importanza e la dignità dell'approccio alla tutela della privacy fin dalla progettazione, ponendo le basi affinché lo stesso diventasse un principio di diritto internazionale.
La risoluzione conteneva una premessa fondamentale su cui si incentrò gran parte del dibattito: il progresso tecnologico pone nuove sfide per tutti gli attori coinvolti nel processo di trattamento, dall'esercizio dei diritti degli individui, alla creazione di nuove e più robuste regole capaci di adeguarsi alle nuove frontiere della tecnologia dell'informazione e della comunicazione.
In ragione di ciò furono approvati i seguenti punti[14]:

1. Riconoscere la Privacy by Design come componente essenziale della tutela della privacy;
2. Incoraggiare l'adozione dei principi fondamentali della Privacy by Design come guida per implementare la privacy come modalità predefinita nei processi di trattamento;
3. Invitare i Garanti e i Commissari per la tutela della Privacy a:
   a. promuovere Privacy by Design il più possibile, attraverso la distribuzione di materiali per il supporto e l'istruzione personale;
   b. favorire l'integrazione dei principi fondamentali della Privacy by Design nella formulazione della regole privacy e della legislazione sulla privacy nelle rispettive giurisdizioni;
   c. incoraggiare la ricerca in modo proattivo sulla Privacy by Design;
   d. considerare di aggiungere la Privacy by Design alle agende degli eventi che si svolgono all'International Data Privacy Day (28 gennaio);
   e. riferire alla 33° International Data Protection and Privacy Commissioners Conference, se del caso,

[9] https://en.wikipedia.org/wiki/Ann_Cavoukian
[10] https://link.springer.com/article/10.1007/s12394-010-0062-y
[11] https://www.schwaab.ch/wp-content/uploads/2013/09/Resolution+on+Privacy+by+Design.pdf
[12] http://globalprivacyassembly.org/wp-content/uploads/2018/11/20181030_Rules-and-Procedures_ICDPPC_October2018-Consolidated.pdf
[13] Dal 1979 si tiene annualmente una conferenza internazionale dei Garanti della Privacy con lo scopo di dibattere intorno agli scenari emergenti in tema di trattamento dei dati personali. Questa conferenza prende oggi il nome di Global Privacy Assembly https://globalprivacyassembly.org/
[14] https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf

sulle attività ed iniziative della Privacy intraprese nell'ambito della loro giurisdizione, al fine di condividere le migliori pratiche.

Nel proseguo degli anni gli studi intorno al concetto di PbD non si fermarono e vennero affrontati - in un'ottica man mano più attenta alla tutela della vita privata degli individui - anche dalla Commissione europea.
Nel 2012 infatti, Parlamento europeo e Consiglio, elaborarono una proposta di Regolamento[15] con riferimento al trattamento dei dati personali in cui, elemento di spicco (almeno per quanto interessa in questa sede), fu proprio la volontà del Legislatore europeo di inserire il concetto di **privacy by design/default** all'interno della nuova legislazione europea, elevando così lo stesso da mera concezione dottrinale, benché riconosciuta a livello internazionale[16], a **principio vincolante** del nuovo assetto normativo europeo in tema di trattamento di dati personali.

3. L'art. 25 del GDPR: "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita"

Nella lettura attualizzata del GDPR, quella del 2016, il principio di privacy by design/default la troviamo all'art. 25:

"Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita"

1. *Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.*
2. *Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.*
3. *Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.*

Nonostante l'articolo risulti abbastanza chiaro nell'esposizione del principio in esame, per comprenderne fino in fondo la portata innovativa non basta una semplice lettura del testo.
Il GDPR infatti pone e impone un nuovo paradigma, pressoché sconosciuto nel panorama giuridico italiano legato al sistema di **civil law**.
Principio cardine del "nuovo approccio alla privacy" è l'"**Accountability**", concetto tipico dei sistemi di **common law** anglosassoni, spesso tradotto come "responsabilizzazione del Titolare del trattamento".
Ed è proprio alla luce di un approccio "**accountable**" che trovano senso le parole dell'art. 25, che, lette in combinato con le altre disposizione del GDPR, in particolare con gli artt. 5 – 6 - 24 – 32 – 35 danno una visione d'insieme di cosa il Legislatore europeo abbia voluto prescrivere con un approccio by design della privacy.

---

[15] Una prima stesura del principio di privacy by design lo troviamo all'Art. 23 della proposta di Regolamento generale sul trattamento dei dati personali, consultabile al seguente link: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52012PC0011&from=CS

[16] La Resolution of Jerusalem costituisce un accordo di principio, vincolante solamente rispetto ai soggetti che l'hanno sottoscritta. (Si rimanda alla nota 12 per l'inquadramento dello status giuridico della conferenza).

Tratto comune degli articoli sopra citati è il fatto che il GDPR prescrive lo stesso approccio basato sul rischio.[17]
Il Titolare del trattamento infatti, dovrà effettuare l'analisi dei rischi legati alle sue esigenze particolari di trattamento, e nel farlo dovrà tener conto di vari fattori, tra i quali: natura, ambito di applicazione, contesto, finalità di trattamento; dovrà tener conto dei rischi per i diritti e le libertà delle persone fisiche, onde garantire (ed essere in grado di dimostrare)[18] l'adozione di misure tecniche e organizzative adeguate[19] alla sua situazione soggettiva.
La "particolarità" dell'art. 25 sta nel fatto che il Titolare dovrà mettere in atto queste misure tecniche e organizzative adeguate – e cita quali possibili misure la **pseudonimizzazione** e la **minimizzazione dei dati** - integrando nel trattamento le garanzie che lo stesso GDPR prescrive a tutela dell'Interessato, e dovrà farlo **al momento di determinare i mezzi del trattamento (design), così che quello risulti il modo in cui i dati vengono concretamente trattati (default).**

L'approccio del GDPR non è tanto un divieto generalizzato di trattare i dati personali, seguito da eccezioni alla regola, tutt'altro. Come si evince dalla rubrica stessa del Regolamento in questione […] "*relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*…", il GDPR si sofferma piuttosto – in un'ottica di generale permesso di trattamento del dato seguito da eccezioni (Art. 9 GDPR) - **sulla sicurezza del dato oggetto di trattamento**, onerando di tale incombenza colui che, nell'ambito delle attività di cui all'art. 2 GDPR, intenda "servirsi" dei dati personali altrui, ovverosia, in primis, il Titolare del trattamento.

3.1. L'art. 25 e l'art.32 del GDPR, breve analisi comparativa

Soffermandosi e facendo un parallelismo, in particolare tra l'art. 25 e l'art. 32 del GDPR[20], si trovano dei punti in comune tra essi, ma soprattutto un approccio alla protezione del dato dell'art. 25 che risulta di principio rispetto all'art. 32 che dispone "il da farsi" nella concretezza del trattamento.

---

[17] L'art. 35 del GDPR impone addirittura una valutazione di impatto (DPIA) allorché un determinato tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

[18] La "responsabilizzazione" del titolare del trattamento viene alla luce fin dal Capo II del GDPR rubricato "principi", in particolare ne troviamo un passaggio all'art. 5 p.2., per poi essere esplicitato al Capo IV relativo al "titolare e responsabile del trattamento" all'art. 24 laddove prescrive esplicitamente che "il titolare mette in atto misure tecniche e organizzative adeguate per **garantire ed essere in grado di dimostrare** che il trattamento è effettuato conformemente al regolamento".

[19] C'è chi: EMEGIAN Fulvia; PEREGO Monica: Privacy & Audit, pagg. 81-82, legge tra le righe dell'art. 32 punto d) GDPR – laddove si prescrive che il titolare del trattamento e il responsabile del trattamento mettano in atto misure tecniche e organizzative adeguate […] che comprendono **se del caso**: "una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento" - un chiaro riferimento all'attività di Audit o ad una procedura ad essa assimilabile, tendente appunto a Testare, Verificare, Valutare le stesse misure di sicurezza.
Se si aderisce a quanto sostenuto dalle autrici, non risulterà allora difficile ricomprendere in questa "procedura" anche l'analisi dei processi di trattamento (misure tecniche e organizzative) che dovranno necessariamente essere implementati Privacy by Design secondo il disposto dell'art. 25 GDPR, inquadrando (si leggerà più oltre nel proseguo della trattazione) l'applicazione del principio PbD stesso come parte integrante della sicurezza del trattamento.
Discorso in parte diverso è invece quello di chi può essere chiamato ad operare l'Audit, in particolare se questo sia un compito che possa essere svolto dal DPO o se si rientri in un'ottica di accountability per la quale spetta sempre al Titolare (ma anche ai suoi consulenti) mettere in atto questa procedura.
A tal fine si ritiene che - per quanto compete in questa sede, dedicata alla trattazione della privacy by design, essendo la stessa una norma cogente, stabilita direttamente dal GDPR - il DPO possa, nell'ambito delle attività che gli sono proprie (art. 39 GDPR) compiere l'attività di Audit anche sul rispetto dell'art. 25, rientrando lo stesso in un'attività di generale sorveglianza sulla conformità al Regolamento europeo.

[20] L'art. 32 può a buon grado considerarsi uno degli articoli più innovativi della nuova disciplina, abbandona – almeno nell'ordinamento giuridico italiano – l'obbligatorietà delle misure di sicurezza minime per abbracciare un approccio alla sicurezza del trattamento basato sul rischio specifico, diverso da struttura a struttura e da trattamento a trattamento, affidando il tutto all'accountability del titolare del trattamento stesso.

Mentre infatti l'art. 32 si concentra nell'indicare che l'onere della sicurezza del trattamento (dall'inizio e nella costanza dello stesso) grava sul Titolare e sul Responsabile, che dovranno ponderare i rischi sulla base della **probabilità** e della **gravità** (**impatto**) del loro verificarsi; l'art. 25 muove da un piano diverso, ad indicare che la sicurezza del trattamento di cui parla l'art. 32 deve però partire da uno stadio preliminare, infatti: pur tenendo sempre in considerazione lo stato dell'arte, i costi di attuazione, l'ambito di applicazione, il contesto e le finalità di trattamento, nonché i rischi aventi gravità e probabilità diverse per diritti e libertà delle persone fisiche, l'adozione delle misure adeguate di protezione dei dati debbono essere adottate – si scuserà la ripetizione - "**sia al momento di determinare i mezzi del trattamento**, sia all'atto del trattamento stesso".
La chiave di volta sta proprio nel fatto che mentre l'art. 32 dispone che siano adottate misure di sicurezza tecniche e organizzative adeguate rispetto ai rischi derivanti dal trattamento, a prescindere da quale sia il "mezzo" utilizzato dal Titolare o dal Responsabile, nell'art. 25 l'attenzione si concentra sul **mezzo** scelto dal Titolare per implementare il trattamento dei dati – e per mezzo si intende l'architettura del processo di trattamento – esso infatti **dovrà essere già sviluppato, ab initio, come compliance al GDPR[21]: non si dovrà cioè implementare la sicurezza come mera sovrastruttura di quel "mezzo" (misura tecnico-organizzativa) che risulta servente al trattamento[22].**

Quell'approccio ex ante alla tutela di cui si parlava sopra e di cui parlano anche le linee guida dell'**EDPB** (European Data Protection Board) – già approvate[23] e in attesa di essere pubblicate dopo la fase di consultazione pubblica - sulla data protection by design and default, e di cui si riportano alcuni passaggi[24]:

"*Article 25 stipulates that controllers should consider DPbDD early on when they plan a new processing operation*".

"*Controllers shall implement DPbDD before processing, and also continually at the time of processing, by regularly reviewing the effectiveness of the chosen measures and safeguards*".

"*The requirement described in Article 25 is for controllers to have data protection designed into the processing of personal data and as a default setting and this applies throughout the processing lifecycle. DPbDD is also a requirement for processing systems pre-existing before the GDPR entered into force. Controllers must have the processing consistently updated in line with the GDPR*".

3.2. Data protection by design, una mera anticipazione di tutela?

Se, come si è detto, l'art. 25 fa onere al Titolare del trattamento di implementare misure atte a garantire la sicurezza del trattamento stesso fin dalla progettazione, considerare però l'approccio "by design" come una mera anticipazione di tutela rischia di non rendere giustizia ad un principio che in realtà è molto più "viscerale" e coinvolge il Titolare del trattamento (in un'ottica di accountability) ad un livello molto più profondo.
Ragion per cui il ruolo del Titolare del trattamento è un ruolo che risulta sì di organizzazione interna, ma soprattutto di verifica e controllo dell'intero processo di trattamento.[25]
Il Titolare quindi, anche alla luce del Considerando 78 al GDPR[26], dovrà vigilare, adottare politiche interne, e attuare misure che offrano effettiva tutela per i diritti e le libertà delle persone fisiche, tendenti a: "*ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire*

[21] Il termine **Compliance** è riferito ad un trattamento che rispetti la "ratio" del GDPR, in particolare, se si vuole, i principi (**finalità; minimizzazione; liceità; esattezza; limitazione della conservazione; integrità e riservatezza**).
[22] L'approccio alla sicurezza del trattamento ex post, cioè quando i dispositivi, se non anche il trattamento stesso, risultano già in essere, è tipico delle tecnologie PETs.
[23] https://edpb.europa.eu/news/news/2020/european-data-protection-board-40th-plenary-session-guidelines-data-protection-design
[24] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf
[25] Nella versione in lingua inglese del GDPR il "titolare del trattamento" è definito come "data controller"
[26] https://www.garanteprivacy.it/documents/10160/0/Regolamento+UE+2016+679.+Arricchito+con+riferimenti+ai+Considerando+Aggiornato+alle+rettifiche+pubblicate+sulla+Gazzetta+Ufficiale++dell%27Unione+europea+127+del+23+maggio+2018

trasparenza per quanto riguarda le funzioni e il trattamento dei dati personali, consentire all'Interessato di controllare il trattamento dei dati […]"

Questa "responsabilità" del Titolare del trattamento però va oltre, e la si ritrova anche allorquando lo stesso si appresti a delegare, anche un solo specifico trattamento, ad un altro soggetto (Responsabile del trattamento).
"*The controller is responsible for the fulfilment of the DPbDD obligations for the processing carried out by their processors and sub-processors, they should therefore take this into account when contracting with these parties*"[27].

L'accordo tra i due infatti dovrà soggiacere a quei precisi requisiti che ritroviamo all'art. 28 GDPR, e questo spiega anche il perché l'art. 25 faccia onere solo al Titolare del trattamento di implementare misure di sicurezza PbD adeguate[28], non essendo assolutamente sufficiente attuare misure generiche solo per cercare di documentarne la conformità.
Le misure tecniche e organizzative infatti devono essere concretamente predisposte alla tutela del dato, cioè dovranno essere adeguate a quel determinato trattamento.

Ma il principio della PbD pur riferendosi direttamente al Titolare del trattamento chiama in causa anche altri soggetti, in particolare gli sviluppatori software che, sebbene non abbiano un dovere guiridico derivante da una fonte legislativa di implementare sistemi che tutelino i dati personali by design, indirettamente risultano coinvolti dalla "normativizzazione" del principio. Dovranno infatti tenere il passo di un'evoluzione della tecnica che ingloberà sempre più gli strumenti di tutela all'interno del prodotto stesso.
Così facendo si mira a garantire la privacy degli interessati durante tutto il ciclo di vita del trattamento, dalla raccolta dei dati al loro "uso", fino alla cancellazione degli stessi.

3.3. Technologies vs law; technologies and law

A questo punto della trattazione, e dando per pacifico che il rischio zero nel trattamento di qualsiasi tipo di dato personale non sia scientificamente perseguibile, possiamo sintetizzare il fine dell'approccio by design alla privacy con una passaggio significativo dell' **EDPS** (European Data Protection Supervisor) estrapolato da un parere - antecedente l'entrata in vigore del GDPR – sulla promozione della fiducia nella società dell'informazione promuovendo la protezione dei dati personali:
"When information and communication technologies are built according to the principle of PbD, the risks to privacy and data protection may be significantly minimized".[29]

Questo nuovo approccio della protezione fin dalla progettazione, si sarà capito, non si limita ad inseguire l'evoluzione tecnologica ma viaggia in "pendant" con essa, per cui - a meno di evoluzioni tanto futuristiche da non poter essere nemmeno pensate in questo momento storico – la tecnologia e la sicurezza del trattamento viaggeranno (l'augurio è questo) sullo stesso binario, indipendentemente dall'evoluzione cibernetica, in quanto i principi della privacy saranno un tutt'uno con lo sviluppo del dispositivo, saranno incorporati ad esso.

Non è ormai più pensabile concepire le regole giuridiche e quelle tecniche come due modelli completamente separati, quasi contrastanti, che si occupano uno di porre le regole di convivenza sociale e l'altro le regole di funzionamento di un apparecchio che proprio nella società troverà il suo campo naturale di applicazione:
"*non è [*più*] pensabile la creazione di due sistemi di regole parallele con fonti separate nel diritto o nella tecnologia, ma è piuttosto concepibile un sistema legale integrato che sfrutti la tecnologia e il suo essere strutturata e strutturabile per rendere più efficaci le norme giuridiche comportamentali*".[30]

---

[27] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

[28] L'implementazione di queste misure tecniche e organizzative, come anticipato nella nota 18, potrà essere oggetto di audit anche da parte del DPO, se nominato.

[29] https://edps.europa.eu/sites/edp/files/publication/10-03-19_trust_information_society_en.pdf

[30] https://iris.unitn.it/retrieve/handle/11572/177733/138944/LawTech_Student_Papers_Bincoletto_Giorgia.pdf

4. I principi fondazionali della privacy by design

La summa delle questioni inerenti il principio di PbD può essere esaustivamente riassunto con l'esposizione dei famosi **7 "principi fondazionali"** formulati da Ann Cavoukian sull'essenza di un approccio "by design" alla privacy[31]:

1. **Proactive not Reactive; *Preventative* not Remedial:** (L'approccio by design anticipa e previene gli eventi invasivi della privacy, non aspetta che I rischi si materializzino);
2. **Privacy as the Default:** (L'approccio by design/default cerca di garantire che i dati personali siano automaticamente protetti in qualsiasi sistema informatico, di modo che gli stessi siano protetti senza che sia necessaria alcuna azione da parte dell'interessato per proteggere la sua privacy);
3. **Privacy *Embedded* into Design:** (La privacy è integrata nell'architettura IT non viene aggiunta al sistema, cioè è una componente essenziale del sistema stesso, senza diminuirne le funzionalità);
4. **Full Functionality—Positive-Sum, not Zero-Sum:** (L'approccio by design è un approccio inclusivo rispetto ad altri aspetti del trattamento, evita le dicotomie, non sacrifica la sicurezza e l'economia per la privacy, ma le implementa entrambe);
5. **End-to-End Lifecycle Protection:** (la privacy, essendo implementata nel supporto atto al trattamento del dato personale, estende la tutela dell'interessato per tutta la durata di vita del dato stesso);
6. **Visibility and Transparency:** (Obiettivi principali della privacy by design sono la trasparenza e la visibilità dell'attività di trattamento nei confronti dell'interessato, che può in qualsiasi momento verificare l'attività di trattamento stesso);
7. **Respect for User Privacy:** (In definitiva, la privacy by design richiede ai programmatori e ai titolari del trattamento di tenere in massima considerazione i diritti degli interessati, offrendo loro tutti gli strumenti per garantire e mantenere il controllo sui dati stessi).

5. Come opera in concreto il principio della protezione fin dalla progettazione: quali sono gli accorgimenti che il Titolare del trattamento deve valutare per garantire (in particolare) un trattamento compliance nell'era dei dati digitali?

Il principio della protezione dei dati personali fin dalla progettazione, non impone tanto delle prescrizioni nuove o ulteriori al Titolare del trattamento quanto, come già detto, la necessità che costui implementi il trattamento di modo che lo stesso risulti già dall'inizio conforme al GDPR.
La conformità al Regolamento europeo però, non è e non può essere una condizione permanente, essa richiede piuttosto uno scrupoloso controllo dell'attività di trattamento stessa da parte del Titolare (**accountability**); questa dinamicità imposta dal GDPR sta anche alla base dell'approccio by design alla protezione dei dati.
Il cambiamento di prospettiva sta proprio nell'adottare un approccio dinamico e abbandonare la staticità del "**semel pro semper**" anche con riguardo ai processi di trattamento[32].
Un approccio "by design" in ottica digitale lo si adotta allora facendo in modo che il dispositivo di trattamento non sia un dispositivo statico, cioè immodificabile, ma sia un dispositivo che possa adeguarsi alle particolari esigenze di trattamento del Titolare stesso.
Con particolare riferimento ai dispositivi tecnologici si può di certo affermare che un dispositivo conformato PbD sia un dispositivo che consente al Titolare o a un eventuale addetto al trattamento (**autorizzato al trattamento**) di **modificare e adattare il sistema** (dispositivo) alle esigenze particolari di trattamento.
Insomma: si interviene sul dispositivo (**design**) per adeguarlo alle esigenze di trattamento (**default**).
Così, per rendere il concetto con un semplice esempio[33]: se un trattamento prevede la raccolta di dati quali nome, cognome, indirizzo mail e codice fiscale per una determinata finalità, e un altro trattamento per

[31] https://link.springer.com/article/10.1007/s12394-010-0062-y
[32] Anche in questo caso "processi di trattamento" deve essere inteso non in ottica prettamente tecnologico-digitale, ma come tecnica di trattamento dei dati a tutto tondo, anche analogica.

raggiungere il fine richiede la conoscenza solamente del nome, cognome e indirizzo mail, il dispositivo deve essere già progettato in modo che la raccolta di queste informazioni (dati personali) da parte del Titolare, possa essere ampliata o ristretta in ottemperanza ai principi del Regolamento, e, in riferimento all'esempio di cui sopra, rispetto al **principio di minimizzazione** di cui fa parola l'**art. 5 p.1 lett. c) del GDPR**.[34]

5.1. Statico vs Dinamico, come cambia l'approccio al trattamento dei dati personali

La distinzione tra un **dispositivo "statico"** e un **dispositivo "dinamico"** sta allora nel fatto che mentre nel dispositivo statico si corre il rischio di richiedere all'utente Interessato la compilazione di spazi già preimpostati dal programmatore, con eventuale riempimento dei campi non necessari alla particolare finalità di trattamento per cui l'Interessato sta fornendo i dati stessi; un dispositivo Pbd compliance consente al Titolare di adattare il dispositivo, di espungere quei campi destinati a contenere dati personali non necessari alla specifica finalità di trattamento, eliminando così la possibilità stessa che il Titolare venga a conoscenza di dati personali ulteriori, in totale spregio al principio di minimizzazione che prescrive, all'opposto, che i dati personali siano: "***adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati***"[35].

Attenzione però che il GDPR è stato sviluppato in modo da essere totalmente neutro rispetto alle modalità di trattamento, siano esse analogiche, digitali o miste. Allo stesso modo l'art. 25 deve quindi essere applicato anche in quei contesti (niente affatto residuali) in cui il dato viene trattato senza l'ausilio di un dispositivo tecnologico; allora il "by design" in questo caso si riferirà in particolare alle modalità organizzative stabilite dal Titolare per implementare il trattamento (ruoli interni, mansioni, modulistica, organizzazione del personale, schedari, autorizzazioni, divieti ecc.).

6. Le linee guida AgID sulla sicurezza informatica: "modellazione delle minacce e individuazione delle azioni di mitigazione conformi ai principi del Secure/Privacy by Design"

L'Agenzia per l'Italia Digitale (AgID) lo scorso 6 maggio 2020 ha emanato una serie di linee guida per lo sviluppo del software sicuro nella pubblica amministrazione.[36]
In particolare l'allegato 4: "*modellazione delle minacce e individuazione delle azioni di mitigazione conformi ai principi del Secure/Privacy by Design*"[37] si occupa di fornire delle raccomandazioni relativamente allo sviluppo e alla progettazione di software e sistemi applicativi sicuri, prendendo in considerazione l'aspetto, tutt'altro che slegato, della sicurezza e della privacy by design.
Senza la pretesa di voler commentare delle linee guida di carattere prettamente tecnico ingegneristico, a cui invece si rimanda per una completezza informativa, si permetta di porre un piccolo accenno a un aspetto importante che si ricava dalla lettura delle stesse:

Nell'ambito delle suddette linee guida, risuona un concetto che apparirà familiare: "**Security by design**".
Infatti, così come la **privacy by design** intende implementare un trattamento dei dati personali sicuro sin dalla fase della progettazione, il concetto di **Security by design** intende definire un software progettato in modo da essere sicuro, cioè in grado di anticipare e minimizzare gli impatti delle vulnerabilità, e di rimando della privacy, garantendo quelli che sono i tre principi alla base di qualunque concetto legato al trattamento di dati, personali e non, e che garantiscono la **sicurezza dell'informazione** nonché il concetto stesso di **sicurezza informatica**:

- **Riservatezza**: con cui si consente l'accesso ai dati solamente agli utenti autorizzati;

---

[33] Si consideri l'esempio in nota come mera esemplificazione pratica, assolutamente non esaustiva rispetto alle molteplici sfaccettature legate alle esigenze pratiche di trattamento.
[34] Beninteso lo stesso esempio lo si può comunque adattare in un trattamento non digitalizzato.
[35] Lo stesso esempio fatto per il principio di minimizzazione può essere adottato, con le dovute differenze, per tutti i principi contenuti nel GDPR
[36] https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro
[37] https://www.agid.gov.it/sites/default/files/repository_files/allegato_4_linee_guida_per_la_modellazione_delle_minacce-dlt.pdf

- **Integrità**: con cui si garantisce la non manomissione o alterazione dei dati da parte di soggetti non autorizzati;
- **Disponibilità**: con cui si garantisce in particolare l'accesso da parte dei soggetti autorizzati o interessati ai dati personali.

7. Considerazioni finali

Il principio di "PbD" lungi dall'essere solo un principio applicabile allo (stretto?) perimetro riguardante la privacy, si muove invece, e sempre di più lo sarà in futuro, in combinato con il concetto di sicurezza.
La pervasività richiamata all'inizio della trattazione non è infatti tanto o solamente una crescente intromissione nella sfera personale altrui di soggetti "desiderosi" (per ovvi ed evidenti fini commerciali e non) di trattare dati personali, ma è una pervasività che rischia di vedere contrapposta la privacy alla sicurezza.
Alla nuova figura del giurista 2.0 allora il compito di far aderire due esigenze che, lontano dall'essere antitetiche, dovranno essere invece la stella polare per una soluzione che non protegga una escludendo l'altra.

Alberto Pittau

#privacybydesign #GDPR #security #AgID #garanteprivacy