Chi, oggi, non utilizza abitualmente la parola "privacy"? Chi non ha lamentato, almeno una volta nella vita, una violazione della propria privacy, anche solo in tono scanzonato e scherzoso?

Al fine di dare una giusta connotazione giuridica, sociale e storica al concetto di "privacy", pare doveroso analizzare tale strumento di tutela della riservatezza dell'individuo attraverso il dovuto parallelismo con il sempre più attuale, ed ulteriore, strumento del "data protection", onde comprendere appieno i significati realistici di questi due "istituti", tracciare la linea di confine tra l'uno e l'altro e dare, se possibile, una giusta classificazione dei loro effetti e delle loro "utilità", cercando anche di fare chiarezza su quelle che sono le loro similitudini o differenze.

Indice

Nascita del concetto di "privacy"

La storia del termine "privacy" desta certamente interesse e curiosità: il primo concetto di *privacy* (come attualmente inteso) prende forma già nell'Antica Grecia. Aristotele ci parla degli impegni pubblici del cittadino e tratta contestualmente anche della sfera privata di questi, ovvero dei risvolti che hanno a che fare con la gestione della vita personale del soggetto all'interno dell'òikos (οἶκος) e, quindi, della casa. Viene, in tal senso, evidenziata l'importanza del potere di esclusione per il singolo, inteso come *ius excludendi omnes alios*, quale diritto e capacità di escludere "tutti gli altri" dai propri spazi personali, assistendo, in tal senso, all'apparizione di una pionieristica formalizzazione di spazio personale, sia esso inteso fisicamente, sia esso inteso quale spazio afferente alle informazioni personali ed alla riservatezza appartenenti all'individuo.

Il concetto di *privacy* richiama, quindi, un altro concetto fondamentale, quello della proprietà privata; concetto che si estende oltre l'ordinario bene materiale (la casa stessa o qualsiasi altro bene proprio) ed oltre, pertanto, l'inviolabilità delle succitate mura domestiche o del bene personale del caso. Esso abbraccia e contempla tutto ciò che appartiene all'individuo, anche la capacità di estrinsecare pensieri propri (e liberi) sino al potere di rivendicare come "assolutamente propri" dati quali il nome, il cognome, l'indirizzo mail (*et similia*) ed addirittura propri pensieri o idee.

La comparsa del "diritto alla privacy" si attesta nel 1890, allorquando negli Stati Uniti il senatore Warren ed il giurista Brandeis "*in un saggio innovativo denunciavano l'intrusione dei giornali scandalistici dell'epoca nella vita privata del primo*"[1]. È qui che assistiamo al perfezionamento del "*right to be let alone*" o, meglio, del diritto (appartenente ad ognuno di noi) "all'essere lasciati soli".

Anche in Europa la *privacy* non tarda a comparire nella sua valenza più profonda e lo fa nel 1909, ad opera del giovane giurista francese Perreau, il quale compone l'articolo "Des Droits de la personnalitè", pubblicato su una celebre rivista di diritto civile. E così, "*Mentre il concetto americano di privacy nasce da un'esigenza di sicurezza personale legata alla proprietà, quello europeo della protezione dei dati personali proviene dal timore che una profilazione dell'individuo possa essere potenzialmente discriminatoria*"[2]. In effetti tale timore non tarda a materializzarsi in Europa: negli anni Trenta, infatti, il governo olandese istituisce un registro anagrafico della popolazione, registro successivamente utilizzato dal regime nazista (il cui esercito invade nel frattempo i Paesi Bassi) onde profilare e scovare tutti gli oppositori, causa le loro origini etniche e religiose[3].

Altrettanto interessante appare la prima "impronta giurisprudenziale" sul tema *privacy* in Italia. Siamo nel 1956 e la Cassazione "dà forma" al tema sulla base del ricorso che i figli e i nipoti del grande tenore Enrico Caruso instaurano contro una casa produttrice di un film che tratteggiava, con importante vigore, la povera estrazione sociale del cantante, ponendo particolare attenzione su alcuni episodi che dipingevano il cantante stesso come vittima di svariate difficoltà economiche tanto da condurlo a propositi suicidari[4].

Tale sentenza traccia il solco italiano tra ciò che è di dominio pubblico rispetto a ciò che riguarda la sfera personale di un soggetto e, quindi, di ciò che deve rimanere necessariamente nell'alveo della riservatezza.

Ancora notabile una Cassazione del 1963, che condanna il settimanale "Tempo" a risarcire i parenti di Claretta Petacci, nota per la sua relazione sentimentale intrattenuta con Benito Mussolini, per avere pubblicato alcuni racconti non di interesse pubblico, bensì afferenti alla vita privata della donna. Anche in tale sede si inizia a dare valorizzazione a ciò che può essere di interesse pubblico e a ciò che non lo è affatto. Bisogna, tuttavia, arrivare alla sentenza del 1975, la numero 2129, per vedere finalmente affermato a pieno titolo il "diritto alla riservatezza/privacy", da parte della giurisprudenza, a credito della moglie dello Scià di Persia, ripresa e fotografata da alcune testate giornalistiche in atteggiamenti intimi con un uomo all'interno delle mura domestiche[5].

---

[1] *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Rocco Panetta - Giuffrè Francis Lefebvre, introduzione, pag. XII.

[2] https://www.agendadigitale.eu/sicurezza/privacy/privacy-e-protezione-dati-personali-cosa-sono-quali-differenze-cosa-e-cambiato-col-gdpr/#post-66738-footnote-ref-2.

[3] Ibidem.

Oggi il GDPR, o meglio il Regolamento Europeo che disciplina la protezione dei dati, al Considerando 51 e al suo articolo 9, presta particolare attenzione proprio alla tutela dei soggetti che possono essere profilati per *"… l'origine razziale o etnica, l'opinione politica, le convinzioni religiose o filosofiche, l'appartenenza sindacale nonché per il trattamento di dati genetici, biometrici, relativi alla salute o alla vita sessuale o all'orientamento sessuale*".

[4] Ibidem.

[5] Ibidem.

In definitiva, possiamo affermare che la storia delle vicende giudiziali che hanno tratteggiato l'avvento della *privacy*, così come oggi conosciuta, sono state tante e tutt'oggi ricevono, più che mai, sempre più cura all'interno delle aule giudiziarie; trovano attenzione da parte dei media e interessano analisi di studio volte a chiarire e a sensibilizzare l'attenzione del cittadino e degli Stati sul tema.

Privacy, Data Protection e GDPR

Il, seppur conciso, racconto storico sull'evoluzione del concetto di *privacy* ci proietta *in medias* ponendo la nostra attenzione su quale sia, innanzitutto, il tratto caratterizzante la differenziazione tra la disciplina, sul tema, nel Vecchio Continente e quella approntata "nel paese dell'avanguardia" quale è da sempre l'America (*rectius*, gli Stati Uniti di America). Quest'ultima, affermatasi nel tempo come la patria del libero mercato e delle transazioni commerciali milionarie, invero, ha fin dagli albori dato particolare attenzione ed importanza alla tutela della riservatezza del cittadino in qualità di proprietario di beni e di consumatore, a differenza di quanto, invece, abbia fatto l'Europa, ove è stata da subito data (già ad opera delle opposizioni alle monarchie, alle dittature ed ai totalitarismi) grande ed importante attenzione al valore della *privacy* come diritto fondamentale dell'individuo.

In tal senso, l'attuale Regolamento Generale sulla protezione dei dati, *rectius* Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, anche conosciuto come GDPR, ha risvegliato gli animi in tutto lo SEE (Spazio Economico Europeo), divenendo anche punto di interesse e di riferimento per tante "nazioni extra-UE", poiché frutto di una storia secolare e di uno sviluppo che, attraverso le vicissitudini dei cittadini europei, hanno portato a risvolti culturali e normativi che, oggi, possiamo definire unici nel loro genere.

In Italia, di fatto, a seguito dell'abrogazione dell'antesignano primo "Testo unico sulla privacy" - la Legge 675 del 1996 - vige tuttora il Codice Privacy, disciplinato dal d.lgs. 196/2003 (così come modificato dal d.lgs. 101/2018), normativa perfettamente adeguata al Regolamento europeo, divenendone quasi "la sua immagine specchiata in patria" in maniera conforme alle realtà giuridiche, politiche, sociali e storiche di essa. Tutto ciò ci dà, pertanto, contezza di come il nostro paese sia perfettamente "al passo con i tempi" o, quantomeno, cerchi di esserlo, nell'ottica di dare sempre più sostanza alla sensibilizzazione, alla tutela ed al valore dello "spazio personale" dell'individuo. D'altronde già Stefano Rodotà, uno dei più eminenti giuristi e politici italiani, nonché una delle menti più brillanti e "più *privacy addicted*" del panorama internazionale (già nominato Presidente dei Garanti della Privacy a Bruxelles nel 2000), "in tempi non sospetti" ci parla appunto di *privacy* in termini di ***sovranità di sè***.

Digital Transformation, da Privacy a Data Protection

Oggi, la *digital transformation* sta dando ulteriormente forma o forse, oseremmo dire, nuova vita al concetto di *privacy* evidenziando in tal senso la dicotomia (almeno quella che cerchiamo di comprendere se effettivamente è tale) tra la *privacy* medesima e il *data protection*.

Infatti, se è vero, *ut supra*, che la *privacy* nasce e riveste la funzione (ontologicamente intesa) di protezione dello spazio personale del *civis*, è altrettanto vero che oggi la stessa *privacy* si manifesta non solo con la necessità di mettere lo spazio privato dell'individuo al riparo da occhi indiscreti, ma si estrinseca anche per mezzo di quelle informazioni e di quei "dati personali"[6] che il soggetto utilizza per ottenere tutta quella serie di beni, aggiornamenti e servizi di cui (oggi più che mai) necessita in qualità di cittadino e di consumatore (da parte dell'azienda o del servizio privato o del pubblico servizio/ufficio). Di fatto il cittadino interagisce quotidianamente con realtà economiche, giuridiche e sociali, sia appartenenti alla sfera privata/commerciale sia a quella pubblica, onde ottenere beni e servizi necessari o accessori.

Il cittadino offre e mette a disposizione i propri dati (o informazioni personali), pertanto, onde poter usufruire di quei beni e servizi senza i quali non potrebbe aderire al consesso sociale o senza cui non potrebbe soddisfare i propri *desiderata*; tali dati, tuttavia, hanno necessità di essere tutelati al pari della "*privacy* ordinaria" e secondo i canoni utilizzati per la difesa di quest'ultima.

Ed infatti, se attraverso il concetto di *privacy* il ruolo dell'individuo diviene quasi quello di soggetto passivo e bisognoso di essere protetto da "aggressioni esterne", ove trattasi di *data protection,* assistiamo al fenomeno secondo il quale il soggetto diviene attore e protagonista della condivisione con terzi di ciò che appartiene alla propria sfera personale. Questi, in tale caso, mette a conoscenza l'*extraneus*, per necessità o per piacere, di ciò che gli appartiene e che risulta essere afferente alla propria sfera più intima.

Spieghiamoci meglio. Il cittadino deve necessariamente, ad esempio, condividere i propri dati con quella porzione di infrastruttura pubblica che, onde rendergli il servizio di cui necessita (pensiamo al semplice ufficio comunale, all'anagrafe, agli uffici di riscossione tributi, al servizio sanitario, etc.), ha bisogno di tutta una serie di informazioni personali (per l'appunto "dati") senza le quali non potrebbe erogare il servizio richiesto (già solo perché, in assenza di quei dati, il cittadino non sarebbe identificabile secondo i protocolli richiesti dall'attuale impianto burocratico). Ora, se è vero che ciò avviene "fin dalla notte dei tempi", è altrettanto vero che la somministrazione dei propri dati in passato non avveniva attraverso strumenti accessibili ed "attaccabili" (*rectius*, hackerabili)[7] da chiunque, bensì avveniva recandosi presso gli uffici competenti per interfacciarsi direttamente e privatamente con il referente dell'ufficio interessato o, magari, inviando in busta chiusa e sigillata, tramite il servizio pubblico delle poste, quanto dovuto.

Od ancora pensiamo a quanto oggi risulti facile, per la maggior parte di noi, condividere in totale libertà proprie informazioni/dati personali su piattaforme *social* (non avendo peraltro contezza - ahinoi! -, nella stragrande maggioranza dei casi, di quali e quanti pericoli si materializzino così agendo) e quanto, ulteriormente, sia comune e facile l'accesso on-line per l'acquisto o l'abbonamento (*ex multis*) di ogni prodotto e servizio quotidianamente offerto dal mercato.

---

[6] Il termine "dato sensibile" appartiene alla precedente ed ormai desueta disciplina.

[7] Pensiamo alla comunicazione dei propri **dati sanitari, riconosciuti dal GDPR come "particolari", somministrati a mezzo dell'uso del personal computer o dello smartphone.**

La trasformazione digitale ha oggettivamente cambiato le cose ed ha cambiato il modo di vivere anche la nostra *privacy*. In effetti l'individuo stesso si è trasformato ed è divenuto il "profanatore" di se stesso, perdendo, in un certo qual modo, quella "sovranità di sé" enunciata dal grande Rodotà. Le motivazioni, chiaramente, sono molteplici ma, in questa sede, non sono analizzabili o "catalogabili". Tuttavia, possiamo quantomeno evidenziare come una delle utilità più performanti introdotte da questa trasformazione (buona o meno che sia, a seconda delle valorizzazioni del caso) sia la **velocità** che ha caratterizzato il cambiamento e che contraddistingue la modalità di comunicazione tra gli interessati[8].

Oggi, oltre ad assistere all'immediatezza (grazie ad Internet) della consegna delle nostre "richieste info-telematiche", tutti noi pretendiamo rapide utilità on-line (anche off-line, *sic*!) da parte del servizio pubblico o privato che sia (poiché oramai incapaci di attendere in un mondo che vuole tutto e subito) e, a loro volta, il pubblico e il privato pretendono da noi immediate informazioni utili a profilarci onde rendere la nostra esperienza di "navigazione" sempre più piacevole e più performante a nostro credito (o almeno questa è la "campagna di Marketing" cui ci siamo abituati al fine di giustificare la nostra volontà/necessità di mettere "in mostra" quotidianamente qualcosa di noi stessi). Esemplificative le capacità e le volontà della stragrande maggioranza degli utenti social (FB, IG, TW, etc.) di consegnare in mano "a sconosciuti" dati personali (talvolta anche particolari)[9] quali informazioni riservate, gusti, preferenze, periodi di assenza dalle proprie abitazioni per vacanza o lavoro, in virtù del desiderio spasmodico di condividere, "*hic et nunc!*", tutto ciò che si fa onde ottenere "più credito sociale".

Ecco! Questo è il punto caratterizzante il *data protection* (e, in questo, si differenzia chiaramente dalla *privacy* in senso stretto), ovverosia essere lo strumento di protezione offerto a chi diviene egli stesso (per necessità o per piacere) divulgatore ed ostensore della propria *privacy*, poiché il dato, fondamento comunque afferente ed appartenente alla sfera più intima e personale dell'individuo, va garantito e tutelato sempre e ad ogni costo (al pari della *privacy*).

Patologie. Incidente di sicurezza e Data Breach

Anche osservando gli effetti patologici derivanti dalla violazione delle strutture volte alla "security" della riservatezza di apparati pubblici, di aziende e del singolo, possiamo ottenere, ulteriormente, quale sia il *discrimen* tra un "sistema Privacy" e un "sistema Data Protection". Infatti, mentre la violazione del primo riguarda ed inficia, in generale, il sistema di sicurezza delle informazioni producendo così un Incidente di Sicurezza, il secondo, invece, riguarda la violazione di uno o più dati (alterandoli, distruggendoli, etc.), producendo, invece, un Data Breach (violazione del/i dato/i).

---

[8] TIC - Tecnologia delle informazioni e delle comunicazioni - ha come suo elemento caratterizzante la velocità a mezzo della quale agisce e funziona.

[9] Pensiamo a chi discute dei propri problemi di salute in chat o in una piattaforma *social*, condividendone con ostentata superficialità, talvolta, documentazione specifica; o ancora all'accesso a siti istituzionali di carattere medico-sanitario a mezzo di connettività non sicure e facilmente hackerabili.

Pertanto, se è sempre vero che ogni Data Breach è un incidente di sicurezza, non sempre un incidente di sicurezza diviene un Data Breach e questo perché "*un incidente di sicurezza non si limita ai modelli di minacce nei quali un attacco viene effettuato ai danni di un'organizzazione dall'esterno della stessa, bensì include anche incidenti derivanti dal trattamento interno che violano i principi di sicurezza*"[10]. E, quindi, parliamo di "incidente di sicurezza" quando trattasi di "eventi endogeni", quali per esempio (*ex multis*): l'erroneo inserimento di dati (di qualsiasi natura) all'interno di un contratto, la non corretta formulazione numerica di indici di riferimento di un'operazione bancaria o il non perfezionamento di una misura tecnica necessaria. Parliamo, invece, di "violazione del dato" quando un evento esterno al sistema (esogeno) mina "l'essenza" del dato stesso; evento esterno che può essere, ad esempio, un attacco cibernetico o, in generale, come già anticipato, un'alterazione, una distruzione, una perdita (*et similia*) dello stesso.

Osserviamo, ancora, come *la violazione del dato*, oltre a generare, ad esempio, distorsioni all'interno dello spazio riservato dell'azienda (pubblica o privata che sia) o dello spazio personale del privato, causi il conseguente generarsi di eventi prodotti da quel Data Breach sul tema "decadimento" della sicurezza fisica e cibernetica degli spazi stessi, portando con sé spesso anche la perpetrazione di reati: dalla "classica" diffamazione (peraltro "aggravata" dall'utilizzo del mezzo social) a tutte le violazioni di dati consumate, ad esempio, dai sex offenders, che si possono tramutare in reati quali lo stalking, il cyberstalking, il revenge porn, l'estorsione, il bullismo e il cyberbullismo, il sex-tortion, ed ancora reati quali quelli afferenti alla violazione della "proprietà info-telematica" come l'accesso abusivo a sistema informatico.

Conclusioni. Sinonimi o "contrari"?

In definitiva, *privacy* e *data protection* hanno la stessa valenza? Sono sinonimi? O sono contrari/in contrasto l'uno con l'altro?

In effetti, giusta quanto fino a questo punto analizzato, possiamo sostenere con serena consapevolezza che essi sono l'uno l'evoluzione dell'altra e, contestualmente, la base reciproca e necessaria alla sopravvivenza di ciascuno dei due. Certamente la *privacy* rappresenta il fondamento storico del *data protection*, mentre quest'ultimo rappresenta la dovuta estensione della *privacy* stessa: la prima, divenendo la finalità necessaria (in ambito privato, aziendale o pubblico che sia) volta alla riservatezza delle informazioni, valorizzandone così la visione teleologica del "secretare" e del non rendere di dominio pubblico ciò che non deve esserlo; la seconda, lo strumento per proteggere effettivamente il dato condiviso, il cui contenuto va effettivamente **minimizzato, pseudonimizzato, anonimizzato, crittografato**, etc. (misure tecniche, queste, formalizzate ed evidenziate dal GDPR, quali *tools* da applicare per la protezione del dato e, quindi, quale esecuzione di ciò che pretende un "sistema *privacy*" degno di tale nome). Di talché, possiamo constatare come l'innovazione introdotta dal GDPR stesso (fungendo da apripista a tutta una serie di normative

[10] https://www.federprivacy.org/informazione/punto-di-vista/data-breach-quale-e-la-differenza-tra-un-incidente-di-sicurezza-e-una-violazione-dei-dati-personali

del settore che auspichiamo possano, sempre più, tutelare la sicurezza del cittadino) sia quella di vedere regolamentato e funzionante, in virtù del "sacro principio della privacy", quell'apparato di tecniche utili ad assicurare la protezione del dato, dell'informazione, della personalità e, in generale, dei diritti fondamentali dei cittadini, nonché la giusta sicurezza fisica e cibernetica degli stessi (in tal senso, oggi, parliamo di Cybersecurity).

Oggi possiamo solo confidare nella capacità degli Stati (primo fra tutti il nostro) di porsi nella prospettiva di disciplinare, garantire, sensibilizzare e tutelare sempre più, e sempre meglio, lo spazio personale del cittadino, inteso e valorizzato quale diritto fondamentale dell'individuo (garantito dalla nostra Costituzione e dalle principali norme internazionali fondate sulle (e per le) libertà degli uomini).

23.01.2023

Avv. Paolo PISANO

Team.O.ne.T
CyberTech Forensic
Security & Investigation

Cofondatore del "Team.O.ne. T.
Cyber Tech Forensic - Torino"

Membro del CTS "Data Security" di ALFAFORM
Socio Federprivacy
Docente in "data protection e cybercrime" c/o la business-school Masterandskills di Roma
Socio aderente presso LAIC: "Laboratorio Avvocati Investigatori Criminologi"