

L'evoluzione del concetto di privacy: dall'oikos al GDPR

In un'epoca dominata dalla digitalizzazione e dalla continua evoluzione tecnologica, il concetto di privacy ha subito profonde trasformazioni, adattandosi alle nuove sfide poste dalla società dell'informazione. Questo articolo, parte di una serie dedicata all'esplorazione dei mutamenti nella protezione dei dati personali, si propone di analizzare il percorso evolutivo della privacy, dalle sue radici storiche fino alle moderne normative come il GDPR.

Privacy nell'era digitale: dalla tutela della vita privata al diritto di essere lasciati soli

Osservandone evoluzioni e vicissitudini giuridiche tra norme *generalis* e *specialis*, nazionali, internazionali o comunitarie, dottrina, giurisprudenza e provvedimenti delle Authority, la privacy appare come un'entità mutevole, da un lato vaga e indeterminata e dall'altro capace di declinarsi, a seconda di esigenze e contesto, in una serie di istanze tutt'altro che nettamente separate ed autonome l'una dall'altra.

Di privacy si parla, sin da subito, in relazione alla tutela della vita privata e familiare – dell'oikos, avrebbe forse detto Aristotele – rispetto alle interferenze di terzi. È la stessa esigenza (to be let alone) di cui parlavano Warren e Brandeis, positivizzata dalla Carta Europea dei diritti dell'uomo all'articolo 8 e nella Carta di Nizza all'articolo 7 e già presa considerazione dalla Corte di Cassazione con sentenza 1652/1994; sostanzialmente un *ius excludendi*, che assume debita rilevanza anche in ambito penale nel delitto di

interferenze illecite nella vita privata.

Il diritto alla riservatezza e le sue applicazioni giuridiche

Soltanto in parte sovrapponibile alla salvaguardia della vita privata, il diritto alla riservatezza è comunque un'ulteriore declinazione della privacy. Tale diritto, come detto, fu riconosciuto a Mrs Pollard ma non a Miss Roberson, nelle rispettive cause legali svoltesi negli Stati Uniti; in Italia, tra gli anni '50 e '60 dello scorso secolo, la Cassazione prima ne negò, con crescente cautela, l'esistenza (così nelle sentenze Caruso e Petacci) [1], per poi tornare sui suoi passi nel 1975 nell'ambito del noto caso Esfandiary:

Il nostro ordinamento riconosce il diritto alla riservatezza, che consiste nella tutela di quelle situazioni e vicende strettamente familiari e personali le quali, anche se verificatesi fuori del domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze che, sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione o il decoro, non sono giustificate da interessi pubblici preminenti.

La riservatezza è collocata in apertura della prima legge italiana sul trattamento dei dati personali ("La presente legge garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale") e, successivamente, viene citata anche dal Codice Privacy del 2003.

Ma è con il GDPR che assurge al rango di principio fondamentale del trattamento dei dati, all'articolo 5 [2], il cui rispetto è notoriamente propedeutico a qualunque altra

valutazione in materia di data protection.

Sempre in merito alla riservatezza, si noti a margine che che, durante l'iter di approvazione del pacchetto di norme comprensivo dell'articolo 612 bis del codice penale, una parte del Parlamento auspicava che alcune di queste norme – tra cui, per l'appunto, quella che prevedeva la punibilità della diffusione di pornografia non consensuale – venissero collocate all'interno di un nuovo ed apposito Titolo del Codice sui delitti contro la riservatezza sessuale [3].

Il diritto all'immagine: tra codice civile e GDPR

Il diritto all'immagine, pur intersecandosi con gli aspetti appena citati, merita un discorso a parte.

Intimamente legato alle origini nordamericane della privacy – palesatasi, come indicato, con l'avvento della fotografia istantanea –, tale diritto è espressamente normato in Italia dall'articolo 10 del codice civile e dalla legge sul diritto d'autore che con gli articoli 96 e 97 si occupa di regolamentare la riproduzione dell'immagine intesa quale declinazione dell'identità personale.

Nella normativa comunitaria non esiste un simile diritto autonomamente considerato, e tuttavia alle esigenze di tutela – presenti e future – sopperiscono le previsioni del GDPR, nella misura in cui l'immagine sia direttamente o indirettamente riconducibile ad un data subject.

All'articolo 9 il Regolamento si preoccupa peraltro di predisporre garanzie di protezione più elevate con riferimento ai dati biometrici, ossia i dati trattati con tecniche che consentono l'identificazione dell'interessato, quali ad esempio il riconoscimento facciale; aspetto, quest'ultimo, ulteriormente approfondito e specificato dall'AI Act adottato

il 24 giugno del 2023 dal Parlamento Europeo.

Sulla scia delle norme e degli orientamenti europei, con il decreto-legge 51 del 2023, l'Italia ha prorogato, almeno fino al 31 dicembre 2025, il divieto di installazione di strumenti di sorveglianza biometrica introdotto nel 2022 dal c.d. Decreto Trasparenza.

Tornando al diritto all'immagine di matrice civilistica, nel definirne i profili di danno l'articolo 10 parla espressamente di "pregiudizio al decoro o alla reputazione", risarcibile a norma dell'articolo 2043 dello stesso codice. La reputazione, come noto, è altresì invocata dall'articolo 595 del Codice Penale in qualità di bene giuridico oggetto di tutela; ed è sempre la reputazione, seguendo ancora una volta il tracciato delle tecnologie dell'informazione, ad accompagnarci sino alla sentenza della Corte di Giustizia dell'Unione Europea (causa C-131/12) del 13 maggio 2014.

Il GDPR e la protezione dei dati personali: un approccio dinamico

Con la sentenza nota come Google Spain la CGUE individuò il diritto all'oblio come autonomo diritto soggettivo, poi ripreso all'articolo 17 del GDPR, allargando l'ambito della reputazione anche al digitale.

E arriviamo proprio al GDPR. Nella "legge privacy" per eccellenza la parola "privacy" non compare neppure una volta, né tra i suoi articoli né tra i considerando, e si presenta piuttosto nella veste di diritto alla protezione dei dati personali, contestualizzato all'articolo 1 come uno dei diritti e delle libertà fondamentali delle persone fisiche.

Quella del Regolamento è un'impostazione decisamente dinamica: il diritto alla protezione dei dati, lungi dall'essere uno statico enunciato, ha implicazioni operative concrete per

tutti i soggetti coinvolti. Leggasi, in merito, a titolo esemplificativo, il primo paragrafo dell'articolo 32 del GDPR:

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

Al titolare (e al responsabile) è richiesto uno sforzo analitico che non si limiti a pesare il rischio in base agli elementi intrinseci e estrinseci del trattamento, ma che sia costantemente rinnovato al variare degli stessi, anche solo per constatare che nulla è variato. D'altro canto agli interessati è accordato un catalogo di diritti dal taglio estremamente pratico. Possono fare al Titolare precise domande o richieste e pretendere una risposta. Nella peggiore delle ipotesi, per attivare lo strumento del reclamo al Garante della protezione dei dati è sufficiente mandare una mail.

A memoria del punto di partenza – lo *ius excludendi*, il *right to be let alone* – ci rendiamo conto che l'approdo del Regolamento europeo segue logiche in parte affini ma non completamente sovrapponibili.

Privacy e protezione dei dati: due concetti distinti ma correlati

A dimostrazione dell'impossibile equiparazione tra tutela della vita privata e il diritto alla protezione dei dati, svedetta l'esempio, peraltro risalente, dell'articolo 4 dello Statuto dei Lavoratori, giacché appare evidente come il divieto di controllo dell'attività lavorativa riguardi la vita lavorativa e non quella intima e familiare[4].

L'esigenza di protezione, per contro, s'incastra perfettamente nei meccanismi del GDPR, e le garanzie del confronto sindacale o dell'istanza all'Ispettorato Territoriale del Lavoro concorrono a realizzare, ante litteram, quel bilanciamento che l'articolo 6 richiede per l'applicazione della base giuridica del legittimo interesse – unica possibile, peraltro, per i trattamenti di videosorveglianza e geolocalizzazione in ambito privato [5].

In merito, anche la Carta di Nizza colloca sfera privata e protezione dei dati in articoli separati (e tuttavia consecutivi): l'articolo 7, già citato, è rubricato "Rispetto della vita privata e della vita familiare", mentre il successivo articolo 8 reca al primo comma: "Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano".

Il leitmotiv: la privacy come diritto al controllo sui dati

Chiudendo il cerchio: ai fini della presente disamina, si è voluto rendere conto, senza alcuna pretesa di esaustività, delle varie specie e sottospecie con le quali la privacy si è presentata e si presenta tutt'oggi. Ma pur a fronte di una tale varietà appare evidente, almeno per chi scrive, che in ognuno dei casi descritti è presente un leitmotiv: il riconoscimento di un diritto dell'individuo ad esercitare un controllo sulle informazioni che lo riguardano.

In tale ottica, la privacy – considerata allora non come termine ombrello o macro-categoria ma, in sintesi, quale diritto al controllo sui dati – somiglierebbe una risposta immunitaria al fenomeno dell'esposizione e diffusione dei dati personali, a sua volta strettamente correlato all'evolversi delle tecnologie dell'informazione.

Così, se all'origine l'anticorpo-privacy si trovava a dover

arginare le modeste sintomatologie causate da stampa a vapore, telegrafo e fotocamera stereoscopica, nel secolo successivo ha avuto a che fare con patogeni ben più virulenti.

Nel prossimo articolo della serie, approfondiremo il tema “Dalla comunicazione mediata dal computer (c.d. CMC) e del primo utilizzo di Arpanet alla ‘biblioteca di Babele’”. Per un’analisi più dettagliata, vi invitiamo a scaricare il white paper di **Marta Zeroni** su **“Sovraesposizione e controllo sui dati personali nell’ecosistema informativo online”**.

Note bibliografiche

[1] Cass. Civ. n. 4487/56: “Nell’ordinamento giuridico italiano non esiste un diritto alla riservatezza, ma soltanto sono riconosciuti e tutelati, in modi diversi, singoli diritti soggettivi della persona; pertanto non è vietato comunicare, sia privatamente sia pubblicamente, vicende, tanto più se immaginarie, della vita altrui, quando la conoscenza non ne sia stata ottenuta con mezzi di per sé illeciti o che impongano l’obbligo del segreto”;

Cass. Civ. n. 990/63: “Sebbene non sia ammissibile il diritto tipico della riservatezza, viola il diritto assoluto di personalità, inteso quale diritto erga omnes alla libertà di autodeterminazione nello svolgimento della vita dell’uomo come singolo, la divulgazione di notizie relative alla vita privata, in assenza di un consenso almeno implicito ed ove non sussista per la natura dell’attività svolta dalla persona e del fatto divulgato un preminente interesse pubblico di conoscenza”.

[2] Articolo 5 paragrafo 1 lettera f) del GDPR: “I dati sono (...) trattati in maniera da garantire un’adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»)”.

[3] BECCARI P., Le prime difficoltà applicative della nuova fattispecie di “revenge porn” in caso di diffusione del materiale da parte di soggetti estranei al rapporto sessuale. Nota a Trib. Reggio Emilia, Sez. GIP/GUP, sent. n. 528/2021 (ud. 09/11/2021, dep. 22/11/2021) in SP Sistema Penale, 6/2022.

[4] In merito, la sentenza Corte App. Milano, Sez. V, 26.2.2014, a fronte di tre casi di registrazioni e/o videoriprese effettuate clandestinamente in ufficio dal datore di lavoro, si è espressa nel senso dell’inapplicabilità dell’art. 4 dello Statuto dei Lavoratori nella misura in cui l’ufficio risultasse “personale” e potesse quindi considerarsi assimilabile a un luogo di “privata dimora”. Per poter estendere la nozione di domicilio al luogo di lavoro dovrebbero ricorrere (almeno) due criteri: la possibilità di esercitare uno ius excludendi nei confronti di terzi e la stabile occupazione del luogo; trova in tal caso piena applicazione l’articolo 615 bis del Codice Penale “Interferenze illecite nella vita privata”.

[5] Provvedimento del 22 febbraio 2018 del Garante per la protezione dei dati personali, Indicazioni preliminari di cui in motivazione volte a favorire la corretta applicazione delle disposizioni del Regolamento (UE) 2016/679 [doc. web n. 8080493].

Profilo Autore



Consulente Privacy e IT Law, auditor, Data Protection Officer e formatrice in materia di protezione dei dati personali e società digitale. Laureata magistrale in giurisprudenza all’Università degli Studi di Padova, con perfezionamento in criminalità informatica e investigazioni digitali alla Statale di Milano e master di secondo livello in Informatica Giuridica presso La Sapienza di Roma.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/articoli/evoluzione-privacy/>