Prefazione

di Raffaele Barberio
Presidente Privacy Italia

L'incontro tra diritto e tecnologia è forse la chiave di lettura più utile per contestualizzare in modo appropriato questo utile ***Dizionario della Privacy*** di Fabio Macaluso e Jacopo Purificati. Gli autori ci offrono uno strumento di consultazione affidabile per addetti ai lavori e non e ne delineano una cornice di riferimento difficilmente comprensibile se non si colloca l'intero settore nella dinamica economica e di mercato delle sue componenti.

1. Ogni epoca storica ha avuto infatti una cifra, una componente di mercato, un fattore della produzione che ha trainato l'economia e ha assicurato crescita e dinamismo. Lo scorso secolo, al di là della sua connotazione tristemente famosa come secolo delle guerre mondiali e dell'olocausto, ha cambiato il mondo.

Per molti secoli e sino all'Ottocento andare dalla Liguria o dalla Calabria a Roma richiedeva circa 4-5 settimane di viaggio in carrozza e 20-25 giorni a cavallo. Poi arrivarono le prime ferrovie, l'auto, l'aereo. Fu scardinato il vincolo dello spazio e del tempo, due categorie che si cominciò a percepire in modo differente. La tecnologia aveva trasferito definitivamente ogni sforzo industriale dal muscolo all'apparato tecnologico.

Ecco perché il Novecento è stato il secolo dell'energia come motore dell'economia. Un secolo in cui tutto, perché funzionasse, andava alimentato con il petrolio o con i suoi derivati. E non è un caso se nello scorso secolo la lettura del potere indicasse la proprietà del mondo nelle mani delle 7 sorelle del petrolio.

Oggi il petrolio non è più il motore del mondo.

Il motore del mondo, ovvero il settore di traino dell'economia, il segmento capace di generare valore più di qualunque altro è quello dei dati.

Alle 7 sorelle del petrolio si sono sostituiti i 5 del GAFAM (Google, Amazon, Facebook, Apple, Microsoft) e ad essi si possono già sin da ora aggiungere i primi colossi cinesi.

La sostituzione del ruolo guida nell'economia dei dati a posto del petrolio ha dato luogo ad una espressione di senso comune quale: "*I dati sono il petrolio del 21° secolo*".

Ma non è cosi, a parte il ruolo di guida trainante dell'economia.

Il petrolio appartiene al mondo delle risorse finite. Può essere usato una sola volta e, quando usato per una volta, si è già trasformato in altro, senza alcuna possibilità di riuso. Avete mai visto qualcuno usare un litro di benzina per andare con il proprio mezzo da una parte ad un'altra e poi una volta arrivato usare lo stesso carburante per ritornare indietro? No, impossibile. Ma c'è di più.

Il petrolio necessita di grandi investimenti per il trasporto (che richiede altro petrolio) e apposite navi che vanno da un continente all'altro per le consegne.

I dati si muovono invece da un capo all'altro del mondo alla velocità della luce e con un costo del tutto irrisorio.

Il petrolio, come dicevamo, può essere usato una sola volta o può essere convertito, ma solo irreversibilmente, in altro come nel caso della plastica. I dati al contrario, più sono usati e più diventano utili, rivelando nuovi valori.

Infine man mano che le risorse fossili diminuiscono, le estrazioni di petrolio diventano più costose e difficili. Al contrario, con i dati la disponibilità aumenta e il costo diventa sempre più irrisorio grazie alla velocità di crescita tecnologica dei computer e dei software.

Il petrolio può avere una sola forma, mentre i dati possono presentarsi, conservarsi e coordinarsi in forma di testo, video, foto, figure e tabelle, idee, fatti, misure, statistiche e qualunque forma che possa essere trasformata in linguaggio binario.

Naturalmente i dati, come il petrolio, sono potere e coloro che controllano i dati si configurano come padroni non solo del mondo, al pari delle 7 sorelle del secolo scorso, ma addirittura dell'universo (Jeff Bezos di Amazon vuole organizzare la conquista di Marte ed Elon Musk di Tesla vuole attivare i servizi permanenti di turismo spaziale).

2. Un altro luogo comune è il sostanziale uso indifferenziato dei termini "privacy" e "protezione dei dati".

La privacy è un concetto forte e antico di secoli, un diritto previsto dalla carta costituzionale ma è anche un termine che oggi non possiamo che ricondurre al principio di riservatezza della persona, al diritto di ciascuno di mantenere vivo il confine di separazione tra la sfera personale propria e della propria famiglia e gli occhi indiscreti dell'opinione pubblica. Ma è anche un concetto che può cambiare in base alla cultura di appartenenza. In Europa, ad esempio, privacy è tradizionalmente un termine che richiama la dignità della persona, mentre in America richiama innanzitutto la capacità di tenere un segreto.

La protezione dei dati presuppone, invece, l'esercizio di proprietà di qualcosa, in questo caso i propri dati personali. Il termine sottolinea ancor di più il valore da proteggere, il fatto che i dati personali rappresentino un immenso valore economico. Un valore che si estrae sia nelle forme di raccolta e custodia dei dati aggregati, si attraverso personalizzazioni ed elaborazioni che vengono effettuate sui dati individuali da strumenti di intelligenza artificiale, capaci anche di esercitare una funzione di predizione sugli atteggiamenti futuri della persona.

Si tratta di dati che animano un immenso mercato globale dove si incontrano

domanda e offerta di dati personali, negoziati all'ingrosso o al dettaglio, in questo caso per aree d'interesse delle persone.

E tutto ciò è avvenuto senza clamori, fintantoché non è scoppiato lo scandalo Facebook/Cambridge Analytica, che ha rappresentato un vero e proprio spartiacque nella consapevolezza dell'opinione pubblica mondiale sul tema.

Da quel momento, conquistando le prime pagine e i telegiornali di tutto il mondo, il caso ha contribuito a diffondere una consapevolezza di massa sul valore dei dati e sul loro uso improprio, prima del tutto inesistente.

L'entrata in vigore del GDPR del 25 maggio 2018, appena due mesi dopo lo scandalo, non poteva avere sostegno di marketing migliore.

Il caso Facebook/Cambridge Analytica ha posto all'attenzione del mondo intero il problema dei nostri dati sui social e della loro raccolta indiscriminata a fini di sfruttamento commerciale o politico.

Abbiamo così scoperto che il mercato di riferimento è servito da un esercito di società che in tutto il mondo raccolgono, organizzano e confezionano i dati relativi alle nostre consultazioni dei siti internet, agli acquisti di ogni genere che effettuiamo in rete, alle relazioni sui social, alle nostre proprietà, ai processi giudiziari cui siamo stati eventualmente sottoposti, al nostro stato civile, ai figli, alla fascia di reddito, alle preferenze politiche, religiose, sessuali e tanto altro.

Queste società registrano tutto ciò che facciamo, raccogliendo e organizzando le tracce che lasciamo dietro di noi, dal momento che ormai quasi tutte le attività sono online.

Un fenomeno che, se effettuato in modo illecito, come spesso è, si interrompe solo quando viene scoperto. E il problema non è l'inefficacia del GDPR. Se il traffico di droga imperversa, nonostante le norme di contrasto al mercato delle sostanze stupefacenti, non vuol dire che la legge non funzioni ma che il valore di quanto trattato è ben maggiore del rischio di essere scoperti.

Naturalmente, la semplice raccolta di questa immensa mole di dati non è sufficiente. È come estrarre il petrolio grezzo. E il petrolio ha bisogno di ulteriore trattamento per diventare benzina e far aumentare significativamente il proprio valore di mercato. E così i dati devono essere trattati con attività di *Analytics*, per essere organizzati e ottimizzati per dare luogo a profili emotivi e comportamentali quanto più possibile affidabili in base ai dati raccolti. Essi sono trattati da software di intelligenza artificiale, che valorizza ogni aspetto del materiale raccolto, collocandolo in un contesto coerente.

In una situazione così composita, appare del tutto evidente come l'entrata in vigore del GDPR abbia creato una sorta di marcia in più sul terreno della protezione dei dati e della tutela delle libertà e della integrità delle persone. Un problema, è evidente, che richiama inequivocabilmente principi fondamentali di democrazia.

Non a caso la stesura e l'approvazione del GDPR hanno richiesto diversi anni. Anni in cui a Bruxelles è stata esercitata, nei confronti delle istituzioni europee, la più grande pressione lobbistica mai registrata al mondo.

Eppure il GDPR è stato approvato e oggi è diventato un modello planetario.

Oltre 130 Paesi hanno adottato negli ultimi tre anni normative di protezione dei dati personali sul modello del Regolamento Europeo.

3. La difesa dei dati personali è e deve essere un compito dello Stato. E lo Stato deve difendere i dati dei propri cittadini allo stesso modo in cui difende i confini nazionali o le proprietà pubbliche. Lo Stato deve farsi carico di questo ruolo perché gli compete in via naturale. E le nostre classi dirigenti devono essere meno distratte in tema di ruolo, peso e sfruttamento altrui dei dati dei cittadini.

Il resto lo mettiamo noi, come cittadini consapevoli dell'importanza dei nostri dati personali, come genitori attenti a proteggere le identità dei nostri figli, come professionisti attenti a indirizzare nella direzione giusta i nostri clienti, come manager efficaci nel posizionamento rispettoso delle nostre attività in linea con la tutela e protezione del consumatore, che è il bene più prezioso per ciascuna azienda.

In questo quadro così composito, Il Dizionario della Privacy di Fabio Macaluso e Jacopo Purificati ci viene in soccorso, perché assicura uno strumento, tanto rigoroso quanto agile, a tutti coloro che, in chiave specialistica o semplicemente per saperne di più, vogliano capire più in dettaglio gli elementi che concorrono alla tutela del dato personale.

Il GDPR è in vigore da oltre due anni e sarà efficace almeno per una decina d'anni, ma già ora in Europa si stanno studiando le possibilità di modifiche in vista delle sempre più presenti applicazioni di intelligenza artificiale e di internet.

Il dato più rilevante è che questa legge è e sarà sotto costante attacco.

Difenderla sarà un problema di dignità della persona, di affermazione dei principi di democrazia, di difesa della sovranità nazionale.

Introduzione

Viviamo certamente nell'era «datocentrica», in un contesto sociale ed economico che ruota intorno allo scambio delle informazioni, siano esse relative alle azioni più semplici e ordinarie della quotidianità (come sfogliare un giornale online a colazione) o allo scambio di larghe masse di notizie fra aziende (anche) di diverse dimensioni.

I dati personali, intesi classicamente, sono le informazioni riguardanti persone fisiche identificate o identificabili attraverso un elemento come il nome o caratteristico della sua identità fisica.

Vi sono anche dati non definibili come personali come, ad esempio, quelli relativi alla portata di una rete elettrica scambiati tra un punto di trasmissione e un altro della stessa rete. Questi ultimi dati sono di grande importanza per il funzionamento del sistema economico: si pensi all'ambiente delle criptovalute (che si avvale di database ad altissimo consumo di energia elettrica, problema di non poco conto), o al traffico internet che si svolge attraverso punti di «interconnessione multipla» a cui le reti degli operatori internet si collegano per scambiare fra loro il traffico IP (su appositi data center).

Come indicato nel *data strategy* dell'Unione Europea[1] del 19 febbraio 2020, «il volume dei dati prodotti a livello mondiale è in rapida crescita, dai 33 zettabyte del 2018 ai 175 zettabyte previsti nel 2025. Ogni nuova ondata di dati offre all'UE grandi opportunità per divenire un leader mondiale nel settore. Anche le modalità di conservazione ed elaborazione dei dati cambieranno significativamente nei prossimi cinque anni. Attualmente l'80% delle elaborazioni e delle analisi dei dati si svolge in centri di dati e strutture di calcolo centralizzate, e il 20% in oggetti connessi intelligenti, quali automobili, elettrodomestici o robot di fabbricazione, e in strutture di calcolo vicine all'utente ("*edge computing*"). Entro il 2025 tali percentuali probabilmente si invertiranno».

La Commissione ha così calcolato che tra oggi e il 2025 vi sarà un incremento nel trattamento dei dati del 530% e che nello stesso anno il volume d'affari

[1] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni "Una strategia per i dati" del 19 febbraio 2020.

complessivo legato alle relative operazioni commerciali sarà pari a 829 miliardi di euro, gli addetti del settore saranno circa undici milioni e il 65% della popolazione europea avrà (almeno) elementari competenze (*skill*) digitali.

Questi numeri, certamente realistici, sono da capogiro e indicano che il tema della privacy e della protezione della vita privata delle persone fisiche è divenuto il mezzo per assicurare il fine economico che la circolazione dei dati garantisce. Questi, i dati personali, come altre materie prime quali il petrolio o il caffè, costituiscono una "*commodity*" che gli utenti mettono a disposizione degli operatori economici allo scopo di godere dei servizi loro offerti a condizioni che in apparenza sono molto vantaggiose o gratuite.

D'altronde, lo stesso Regolamento generale sulla protezione dei dati ("GDPR") indica testualmente che «la libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alle persone fisiche», con ciò gonfiando le vele delle aziende che basano le loro attività attraverso l'utilizzo di questi beni preziosi.

Ciò è riscontrabile, ad esempio, osservando la condotta dei grandi operatori della rete (gli "OTT" come Amazon, Google, Apple, Facebook, ecc.), che si mostrano quasi remissivi di fronte ai regolatori che dettano il quadro di tutela della vita privata (andrebbero fuori mercato se si contraddicesse il principio generale della circolazione dei dati appena detto), mentre sono più aggressivi a protezione di altri versanti dei propri mercati (si pensi solo alle "barricate" erette per depotenziare la recente Direttiva in materia di copyright[2] che per gli OTT può minare l'approvvigionamento dei contenuti d'autore caricati sulla Rete).

La composizione degli interessi in un settore così promettente dà alla materia un grosso risalto mediatico. Il Garante Privacy italiano ha ormai maggiore esposizione rispetto alle altre autorità indipendenti (a tutela della concorrenza o delle telecomunicazioni), poiché sono in gioco princìpi sanciti costituzionalmente (come quelli della segretezza della corrispondenza, della salute o della libertà di pensiero) che sono fondamentali per la vita dei cittadini. Si pensi solo ai frequenti interventi del Garante relativi alla gestione pubblica della pandemia da Covid-19, che si è concretizzata in propri provvedimenti e indicazioni che hanno mitigato l'"intrusione" nelle sfere private degli individui attraverso norme pervasive e applicazioni tecnologiche di tracciamento.

Cionondimeno, la diffusione di *news* riguardanti la tutela della privacy, a parere di chi scrive, non ha aumentato la consapevolezza degli interessati (gli individui che cedono i dati) in ordine ai propri diritti. Ciò per tre motivi: 1) la normativa in questa materia è molto articolata e frammentata in decine di fonti. La lettura e interpretazione delle sue norme (molte di natura strettamente tecnica) costituiscono una riserva per esperti giuridici e informatici, mentre i lettori comuni vengono normalmente frustrati quando si accostano a una tale congerie di disposizioni; 2) le informative sul trattamento dei dati personali e le richieste di consensi e di accettazione di *cookie* sono talmente numerose che esse vengono frequentemente

[2] Direttiva 2019/790 sul diritto d'autore nel mercato unico digitale.

ignorate dalle persone che vengono sopraffatte da una "valanga" di documenti dal contenuto pedissequo e sovente poco intuitivo; 3) la distanza tra il fornitore del dato personale e il soggetto economico che lo utilizza è talmente ampio che l'individuo perde interesse nei confronti delle informazioni che alimentano il circuito produttivo, essendo escluso dalla percezione di vantaggi economici diretti legati al conferimento dei propri dati all'industria.

La Commissione, con la sua comunicazione al Parlamento europeo e al Consiglio del 24 giugno 2020, ha fatto il punto dell'applicazione del GDPR a due anni dell'avvio della sua applicazione. Eloquente l'inciso nel titolo della medesima: «la protezione dei dati come pilastro dell'autonomia dei cittadini e dell'approccio dell'UE alla transizione digitale».

In effetti, la disciplina dettata dal Regolamento è molto evoluta e, come avanzato dalla Commissione nella sua comunicazione, «costituisce una componente importante dell'approccio alla tecnologia incentrato sulla persona nonché la bussola per l'impiego della tecnologia nel contesto della duplice transizione, ecologica e digitale, che caratterizza la definizione delle politiche dell'UE», aggiungendo che esso è «uno strumento essenziale per garantire che le persone dispongano di un migliore controllo sui loro dati personali e che tali dati siano trattati per una finalità legittima, in maniera lecita, corretta e trasparente».

Considerazione che non può che condividersi, tenuto anche conto che diverse imprese che operano a livello mondiale hanno autonomamente deciso di offrire il livello di protezione garantito dal Regolamento anche nei territori in cui esso non trova applicazione.

Ciò fonda la sua logica in una radice di natura commerciale: offrire servizi e prodotti in una cornice effettiva di garanzie costituisce un *asset* concorrenziale molto interessante che, se ben comunicato, può invogliare i consumatori a preferire l'operatore economico che presti tali accorgimenti. A questo riguardo, come notato dalla Commissione, il diritto alla portabilità dei dati assume importanza decisiva per «mettere le persone fisiche al centro dell'economia dei dati consentendo loro di passare da un fornitore di servizi a un altro, di combinare servizi diversi, di utilizzare altri servizi innovativi e di scegliere i servizi maggiormente rispettosi della protezione dei dati», con ciò favorendosi il gioco della concorrenza.

Di contro, l'applicazione del Regolamento nel territorio europeo non è nei fatti uniforme e sconta differenze culturali e di scuole giuridiche.

Formuliamo questa osservazione avendo esaminato il rapporto annuale di DLA Piper relativo alle violazioni dei dati personali ("*data breach*") nel territorio dell'Unione pubblicato a gennaio 2020[3]. Il *data breach* è un evento particolarmente delicato che può causare la perdita dei dati o la loro divulgazione non autorizzata: in tal caso, il titolare del trattamento (la persona fisica e giuridica impresa o l'autorità pubblica o altro soggetto singolo che svolge il trattamento dei dati) è tenuto a notificare l'incidente all'Autorità di controllo (in Italia, il Garante Priva-

[3] "DLA Piper GDPR data breach survey: January 2020".

cy). Leggendo il rapporto, desta una certa meraviglia lo iato nel numero delle notifiche tra paesi come l'Olanda e l'Italia, rispettivamente al primo e al terzultimo posto per numero di *data breach* per ogni 100.000 persone. Difatti, dall'entrata in vigore del Regolamento nel maggio 2018 fino al gennaio 2020, in Olanda sono state notificate 40.467 data breach all'Autorità di controllo, contro i 1.886 al Garante italiano.

Ciononostante il nostro Paese è appena al di sotto di Francia e Germania per la misura delle sanzioni pecuniarie irrogate dalle Autorità di controllo nei distinti Stati nel periodo indicato, ben al di sopra dell'Olanda.

Non è quindi peregrino affermare che l'applicazione del Regolamento non proceda su binari uniformi, a causa dell'interpretazione diseguale dei suoi destinatari (interessati, titolari e responsabili del trattamento) e delle stesse Autorità di controllo che, nonostante le funzioni di indirizzo svolte dal Comitato europeo per la protezione dei dati, possono assumere decisioni diseguali per casi simili.

Non è pertanto un caso che la Commissione, nella sua comunicazione del 24 giugno 2020, abbia annunciato l'istituzione di una "Accademia sulla protezione dei dati", definita come «una piattaforma nella quale le autorità di protezione dei dati dell'UE e straniere possano condividere conoscenze, esperienze e migliori pratiche con l'obiettivo di facilitare e sostenere la cooperazione tra le autorità preposte a far rispettare le norme in materia di tutela della vita privata».

L'auspicio è che tale Accademia sia un luogo di riflessione e non uno strumento di moltiplicazione di atti che stratificano ulteriormente il sistema di norme in materia di privacy.

Questo dizionario nasce dall'esigenza di orientarsi in una materia così composita e complessa.

Le fonti della disciplina a tutela della vita privata delle persone discendono dal Regolamento; vanno altresì menzionate altre norme di rango europeo (come la Direttiva ePrivacy, che presto si trasformerà nel corrispondente Regolamento), il Codice Privacy e altre norme di diritto interno, i codici di condotta ai sensi del Regolamento e le regole deontologiche varate dal Garante, le linee guida dell'*European Data Protection Board* (il Comitato Europeo per la protezione dei dati), i provvedimenti delle autorità nazionali, gli standard tecnici adottati da istituti come l'Agenzia europea per la cybersicurezza ("ENISA"), le prassi consolidate e i contratti tipo. A queste fonti si aggiungono norme di diverse natura e funzione, come, solo per citarne alcune, quelle a tutela dei lavoratori o della libertà di espressione.

Va anche osservato che la materia è dominata dall'elemento tecnologico, stante il continuo sviluppo delle tecniche digitali che rendono massiva la raccolta dei dati personali e lo svolgimento di operazioni di trattamento e profilazione.

La dispersione delle norme non agevola il lavoro di ricerca degli operatori della materia (per fini professionali o scientifici) e tende a scoraggiare chi vi si avvicina in maniera occasionale. Di conseguenza, è quantomeno problematico per l'interessato (l'individuo di cui si tutelano i diritti) comprendere il contenuto del

Regolamento, tanto più che la sua traduzione italiana non è sempre adeguata. Del pari, è arduo per i titolari o i responsabili del trattamento, che in base al principio di responsabilizzazione (*accountability*) sono tenuti a mettere in atto misure tecniche e organizzative adeguate (dimostrando di averle approntate), garantire che il trattamento sia effettuato correttamente. Per questo abbiamo semplificato la lettura delle disposizioni in materia (da ogni fonte provenissero), formando un dizionario suddiviso in 53 voci, ognuna dedicata a un tema specifico che inquadra sinteticamente i suoi temi essenziali. Esse sono esposte in ordine alfabetico, dalla prima, dedicata agli Amministratori di sistema, all'ultima, in ordine alla Violazione dei dati personali[4].

Abbiamo adottato un approccio essenziale, presentando ogni voce con un'esposizione completa, segnalando (laddove presenti) le relative criticità interpretative e applicative, le norme a esse collegate e indicando le figure comuni, professionali e aziendali cui è "dedicato" e particolarmente rivolto l'argomento trattato.

Attraverso questa compilazione, il quadro della materia è stato ricostruito sia in maniera definitoria che in termini "dinamici", perché le voci del dizionario sono sia collegate tra di loro che seguite da un glossario dei lemmi più rilevanti nella materia.

Ci auguriamo che questo volume possa rappresentare un utile riferimento per gli interessi e le attività del lettore.

[4] Nel testo, il termine "Regolamento" sta per *Regolamento generale sulla protezione dei dati* (abbreviato nell'acronimo comune "GDPR"); il termine "Codice" sta per il D.Lgs. 30 giugno 2003, n. 196, novellato con D.Lgs. 10 agosto 2018, n. 101, recante il *Codice in materia di protezione dei dati personali*; il termine "Garante" sta per *Garante per la protezione dei dati personali*.