Evoluzioni della GDPR: problemi e opportunità

Giorgio Merli, autore di numerosi libri e articoli sul Management pubblicati in Europa e negli Usa, consulente di Multinazionali e Governi, docente in diverse Università in Italia e all'estero. Già Country Leader di PWCC e di IBM Business Consulting Services

Cosa sta succedendo nel modo del business dei dati? Tim Cook, CEO di Apple, ha iniziato pochi giorni fa la sua guerra contro gli altri grossi gestori di dati (Google&c) con l'accusa di eccesso di violazione della privacy dei cittadini. Si tratta di un business che solo in Europa vale già 325 Miliardi di Euro (2.6% del PIL) e che si prevede varrà più di 550 miliardi nel 2025 (Commissione Europea,*The European Data Market Monitoring Tool,* 21 gennaio 2021*).* Il contesto normativo si sta dimostrando decisamente inadeguato a regolamentarlo. Si consideri infatti che tale business si basa prevalentemente sui dati personali dei cittadini, sollevando il problema della privacy e dello sfruttamento di tali dati senza alcun riconoscimento del valore ai legittimi proprietari. Il tema sta diventando molto caldo anche in Europa (specialmente in Germania e regno Unito), nonostante siamo stati i primi nel mondo a tentare di regolamentare tale business. Quali evoluzioni si possono prevedere a riguardo? Il regolamento europeo su privacy e dati (GDPR = *General Data Protection Regulation*), operativo dal 25 maggio 2018, infatti si dimostra già inadeguato sia per gli scopi per cui era stato attivato, sia per le modalità previste. Infatti la GDPR prevede che la divulgazione e l'uso dei nostri dati personali da parte delle imprese che li ottengono/detengono possa avvenire solamente attraverso l'ottenimento di liberatorie (i ben noti "consensi"). L'utilizzo della logica dei consensi si è rivelata in realtà molto poco "tutelante", in quanto il cittadino/cliente li concede senza essere ben consapevole delle implicazioni, spesso superficialmente o per poter procedere nella navigazione sui siti internet o perché proposti in modo non molto chiaro. I dati cui tale regolamentazione si riferisce sono inoltre quelli che venivano di fatto considerati nel 2018, cioè dati di tipo "statico", quali nome, indirizzo, targa dell'auto, ID, ecc… Si tratta di dati che vengono poi utilizzati come "*Data Set"* (ad esempio dati sui consumi elettrici settimanali) per tutte le analisi utili ai fini commerciali, sanitari, sociali e altro. L'esplosione dell'uso degli SmartPhone, delle App e *dell'Internet of Things (IoT)* sta però ora producendo dati ben più interessanti per il business (ma anche per usi sociali e sanitari), cioè "dati dinamici", che rappresentano informazioni su spostamenti e comportamenti. Non si tratta più di semplici Data Set, ma di flussi di dati in tempo reale ("Data stream"), che forniscono ad esempio informazioni sugli spostamenti fisici ma anche sulle nostre navigazioni in Internet (i "comportamenti" in senso lato). Per questa tipologia di dati, molto intrecciati come responsabilità tra operatori telefonici, gestori degli smarthphone, app di geolocalizzazione e di tutti i tipi, occorre ora una diversa e maggiore attenzione, non contemplata dalla GDPR. Sono in corso importanti discussioni a riguardo (ogni giorno la stampa ne riporta qualcuna). La Commissione Europea è ben conscia dell'attuale inadeguatezza normativa. Ma è altrettanto conscia che non è possibile tenere sotto controllo gli imprevedibili sviluppi delle tecnologie digitali sviluppate per nuovi business basati sul valore dei dati. Il tutto nel contesto della diffusione in corso dell'uso delle Blockchain e delle Criptovalute, che pongono ulteriori problemi e complicazioni a riguardo. Occorre quindi trovare un modo più efficace per garantire al cittadino/utente/cliente una tutela adeguata sull'uso dei suoi dati personali da parte di terze parti. Occorre prendere atto che il concetto di "privacy dei dati" è di fatto superata nella nuova realtà, in quanto concepita all'era "pre-Internet", quando i dati personali erano un insieme di informazioni statiche (dati anagrafici, ID, consumi, ecc..). Si prevedeva inoltre che questi dati sarebbero stati utilizzati per un insieme limitato di servizi e da un numero limitato di parti (datori di lavoro, banche, assicurazioni, servizi pubblici, medici, ecc..). L'obiettivo delle normative era proteggere questi set di dati dall'utilizzo da parte di terze parti non autorizzate. Ciò doveva avvenire principalmente garantendo che i repository di dati statici non fossero vulnerabili ad attacchi esterni e attraverso garanzie contrattuali da parte delle Organizzazioni utilizzatrici. I dispositivi connessi a

Internet (smartphone, telematica automobilistica, contatori di energia intelligenti, dispositivi indossabili), stanno però ora trasformando i nostri assets e noi stessi in *digital twins* (gemelli digitali di noi stessi) che producono flussi di dati che descrivono puntualmente il nostro stato e i nostri comportamenti. La disponibilità di questa quantità di informazioni è senza precedenti e consente alle aziende e a ogni tipo di organizzazione di fornirci servizi sempre più innovativi, quali ad esempio il monitoraggio dei rischi per la salute e la sicurezza, la fornitura di servizi basati sulle tipologie di consumo, la guida autonoma, ecc. In questo nuovo contesto dovremmo ora essere messi in grado di decidere unilateralmente quale di queste parti possono avere accesso ai flussi di dati generati dai nostri dispositivi e dovremmo essere messi in grado di cambiare idea in qualsiasi momento (ad esempio concedendo l'accesso ad alcune parti e revocandolo ad altre). **Come ben sappiamo oggi non è così.** I nostri dati (praticamente tutti, compresi quelli sanitari e finanziari) sono attualmente di fatto a disposizione e usati dai big player di Internet per fini non sempre ben esplicitati al momento della sottoscrizione di un loro servizio. Di ciò siamo complici inconsapevoli noi stessi quando diamo superficialmente i nostri consensi a proposte di servizio e specialmente accettando alcuni cookies durante la nostra navigazione in internet. Stiamo purtroppo scoprendo ora che tali dati spesso vengono usati anche in modo illegale dalle aziende che li detengono o ne vengono in possesso (si pensi alle recenti sanzioni comminate a diversi operatori telefonici). Esiste inoltre, purtroppo, anche un mercato nero, operante prevalentemente nel Dark Internet, dove i nostri dati vengono venduti al miglior offerente o a chiunque (si pensi alla recente notizia di una proposta apparsa in internet di un set di oltre un milione di dati personali offerti alla cifra di 450€ a chiunque li volesse). Come conseguenza dell'adozione diffusa di dispositivi connessi che generano flussi continui di dati, **la tutela della privacy è diventata dunque praticamente impossibile**. Il focus normativo e tecnologico è quindi costretto a spostarsi dal velleitario obiettivo di tutela della privacy attraverso la protezione del database contenente i set dei dati generati dai nostri dispositivi (contatori, black-box, smartphone, ecc..) alla protezione dei dati alla fonte, cioè prima di ogni possibile intervento da parte di terzi. Ciò significa poter intervenire nel momento della generazione del dato, direttamente nel dispositivo che genera il flusso dei dati stesso. Si tratta di passare dal concetto di “Privacy dei dati” (cioè protezione dei set di dati dall'accesso da parte di parti non autorizzate) al concetto di “Proprietà dei dati” (che implica la facoltà/diritto di concessioni e revoche da parte dei generatori/proprietari dei flussi di dati). Questo concetto diventa quindi centrale nel tema della portabilità dinamica dei dati, come descritto dalla Commissione Ue (COM (2020) 66 def., pagine 10 e 11), dove si recita: "Le nuove tecnologie digitali decentralizzate come la blockchain offrono un'ulteriore possibilità per le persone e per le aziende di gestire i flussi di dati e il loro utilizzo, sulla base della libera scelta individuale e dell'autodeterminazione. Tali tecnologie renderanno possibile la portabilità dinamica dei dati in tempo reale per privati e aziende, insieme a vari modelli di remunerazione per il loro utilizzo". A tal fine occorrerebbe promuovere lo sviluppo di un sistema operativo europeo di tipo “open source”, che possa garantire quanto descritto, e cioè che la proprietà dei dati venga assicurata sin dal punto di generazione dei flussi di dati, cioè dai nostri dispositivi connessi. Ciò significa **decentralizzare** il controllo dell’accesso ai dati (che oggi è invece centralizzato nei Market Place gestiti dai big Player di Internet), rimettendolo nelle mani dei legittimi proprietari – i cittadini/utenti – che potranno personalmente concedere e revocare il consenso all’utilizzo degli stessi a terze parti. In tale configurazione l'unico ruolo di un data hub centralizzato che riceve dati da dispositivi connessi dovrebbe essere quello di un broker "cieco", vale a dire uno strumento che ha la sola responsabilità di distribuire dati crittografati, senza avere visibilità su di essi, né la possibilità di raccoglierli. Questi "mediatori ciechi" sono gli "intermediari dei dati" neutri descritti nel Reg.COM (2020) 767 def., cons 22. Gli intermediari dei dati dovrebbero essere semplici fornitori di servizi di condivisione degli stessi, essendo indipendenti sia dai titolari dei dati che dagli utilizzatori. Hanno come obiettivo principale la creazione di un business, di una relazione giuridica, e potenzialmente anche tecnica, tra i proprietari dei dati da un lato e i potenziali utilizzatori dall'altro (eventualmente con *smart contracts* in blockchain). Assistono entrambe le parti in una transazione di asset di dati, con l'obiettivo di intermediare tra un numero indefinito di titolari di dati e di utilizzatori di dati”. Chiaramente non è oggi così per gli attuali sistemi operativi mobili, che consentono invece ai loro proprietari, ad esempio

Alphabet e Apple, di avere piena visibilità su tutti i dati generati dai sensori presenti nei nostri smartphone. I giganti tecnologici americani e cinesi stanno già “monetizzando” largamente i nostri dati, senza coinvolgerci nella catena del valore del dato (cioè senza riconoscerci nulla a fronte di quanto guadagnano usando e/o vendendoli). Si pensi che le aziende quotate con maggiore capitalizzazione sono attualmente le aziende che basano il loro business sui dati (Alphabet, Google,Tesla, ecc…). L’UE, al fine di dare alle nostre imprese la possibilità di competere anche esse su questo mercato, dovrebbe quindi aggiornare le proprie politiche decentralizzando i diritti di monetizzazione dei dati, consentendo cioè ai legittimi proprietari degli stessi di cederli in cambio di servizi o cashback o tokens. Le imprese dell'UE avrebbero così la possibilità di creare i propri hub di scambio di dati, in cui i loro clienti business e retail potrebbero condividere liberamente i flussi di dati generati dai dispositivi connessi con i partner commerciali della Società in cambio di servizi o altro. Le grandi società genererebbero ricavi dalla gestione di tali hub di scambio di dati – con percentuali sulle transazioni -, moltiplicando così il valore dei loro investimenti IoT (ad esempio nei contatori intelligenti o nella telematica automobilistica). Le PMI avrebbero un accesso senza precedenti a flussi di dati in tempo reale, che sono dati di grande valore. Tali hub di scambio di dati costituirebbero quei “pool di dati interoperabili a livello nativo” descritti dalla Commissione europea nel documento di cui sopra.” Per fare quanto auspicato occorrono nuove piattaforme tecnologiche capaci di far gestire l’utilizzo dei flussi di dati (con criptazione end-to-end), direttamente da parte del proprietario/produttore degli stessi. In questo modo egli può scegliere tra gli utilizzatori a lui proposti dal broker gestore dell’Hub e poi gestirli attraverso una logica dinamica di *grant&revoke* a fronte dei benefici che gli vengono dati in cambio. Tali piattaforme sono ancora rare, ma val la pena di notare che la più avanzata a riguardo è probabilmente quella sviluppata da una start up italiana (Ecosteer), che ha già ottenuto brillantemente e velocemente un Patent negli USA (in soli due mesi, a riprova dell’interesse mondiale a riguardo e della bontà della soluzione).