IL SOLE 24 ORE RAPPORTI

Data: 16.05.2022 Pag.: 9
Size: 369 cm2 AVE: € .00
Tiratura:
Diffusione:
Lettori:

Orizzonte complesso per la difesa dei dati nel mondo virtuale

—D. Aq.

Privacy

Il 25 marzo scorso la presidente della Commissione europea, Ursula von der Leyen, e il presidente degli Stati Uniti, Joe Biden, hanno comunicato un nuovo accordo preliminare sul flusso di dati transatlantico. Un'intesa "di principio" che lascia sperare gli operatori. Mentre prosegue il vuoto normativo aperto nel luglio 2020, quando con la sentenza "Schrems II" la Corte di Giustizia Ue invalidò la decisione della Commissione sull'adeguatezza del "Privacy Shield" (decisione adottata a sua volta in seguito alla caduta dell'accordo "Safe Harbor"). Il giudizio della Corte in sintesi: quel trattato non forniva sufficienti garanzie, da parte statunitense, sul rispetto dei dati europei.

«Per ora c'è la cornice, ma mancano i contenuti (pare che il possibile accordo possa arrivare per fine anno, *ndr*). Nel frattempo si continua a navigare a vista», osserva Alessandro Vercellotti, fondatore dello studio **Legal For Digital**. «Oggi tutti i nostri principali strumenti digitali sono made in Usa e non andrebbero bene in caso di trasferimento dati. Per le nostre aziende sarebbe praticamente impossibile lavorare, basti pensare all'importanza di Google Analytics per i portali online. O alla diffusione delle piattaforme di mailing e marketing. E dunque si prosegue applicando le raccomandazioni europee per garantire una protezione sostanzialmente equivalente a quella Ue, ma aspettando una soluzione definitiva del problema».

Le aziende attendono questo nuovo accordo «perché continuano a essere esposte a ingenti sanzioni. E nell'ambito della protezione dei dati personali il trasferimento all'estero rappresenta sicuramente un tema caldo nel breve termine – precisa Vincenzo Colarocco, avvocato dello studio **Previti** e responsabile del dipartimento "Compliance, media e tecnologia" –. Ma ci sono sul tavolo anche altre questioni irrisolte, legate al mondo del digital advertising, specie dopo l'entrata in vigore, il 10 gennaio scorso, del nuovo provvedimento del Garante ("Linee guida cookie e altri strumenti di tracciamento", *ndr*)». Il provvedimento è stato preso per aiutare l'utente nella gestione dei cookie di profilazione o proseguire la navigazione solo con quelli tecnici, necessari al funzionamento del sito. E anche per evitargli la cosiddetta *"cookie fatigue"*: la frustrazione generata dalle continue richieste di consenso all'uso. «All'atto pratico, però, se si rifiuta ogni consenso, gli editori non riescono a inviare pubblicità profilata ma neanche generalista. E ciò potrebbe portare a un cambio delle loro politiche di business, virando ad esempio verso l'offerta di notizie a pagamento», aggiunge Colarocco.

Il nodo, insomma, resta sempre quello della *data monetization*. E ad altri livelli la sfida si farà più complessa, ricorda Colarocco: «Stiamo già assistendo, ad esempio, alla tokenizzazione dell'uomo, a chi crea un Nft di se stesso. E non solo. I metaversi implicano infatti l'uso di dati particolari, come quello biometrico: e lì si prevede un altro terreno di confronto con Usa e Cina. Senza contare gli altri interrogativi posti dall'uso della *blockchain*: come garantire il diritto all'oblio, visto che il dato immesso è immutabile e non può essere cancellato?».

La privacy è materia viva. E sul digitale è sotto continuo attacco, anche fuor di metafora. Sul terreno della *cybersecurity* si gioca la credibilità delle aziende, anche se – sottolinea l'avvocato Vercellotti – «ci sono vari livelli di attacco e il punto da cui partire è il fattore umano, la formazione, perché ci sono dipendenti che hanno difficoltà a individuare anche solo il *phishing*. C'è ancora tanta strada da fare, considerando che spesso le aziende investono in sicurezza solo dopo aver subito un attacco o dopo che un diretto competitor è stato colpito».

Il tema, più in generale, è di tipo culturale e riguarda tutti i profili della compliance. Ne è convinto Giuseppe Di Masi, socio dello studio legale **Sza**: «Gran parte delle aziende, soprattutto medio-piccole, non ha ancora piena consapevolezza che la compliance e quindi anche le questioni della privacy e della sicurezza informatica sono parte integrante del business. Gli investimenti non dovrebbero avvenire a posteriori ed essere guidati dal timore di nuovi attacchi, ma dovrebbero essere visti come opportunità di crescita, che interseca diversi piani e settori».

Ecco perché, secondo Di Masi, «per le imprese è necessario un sistema integrato di compliance, che guardi alla sicurezza informatica, ma anche alla 231, all'antiriciclaggio, all'implementazione dei sistemi Iso. Si eviterebbero così molti *data breach* con tutte le loro dannose conseguenze. Ma si eviterebbe anche che, come spesso accade, le violazioni vengano denunciate solo quando l'impresa è messa spalle al muro».

Sul terreno della cybersecurity si gioca anche la credibilità delle aziende, chiamate a investimenti preventivi

IL SOLE 24 ORE RAPPORTI

Data: 16.05.2022 Pag.: 9
Size: 369 cm2 AVE: € .00
Tiratura:
Diffusione:
Lettori:

LE TESTIMONIANZE

I metaversi implicano l'uso di dati particolari, come quelli biometrici. E c'è il problema di garantire il diritto all'oblio nella blockchain, visto che il dato immesso non può essere cancellato

Vincenzo Colarocco
Avvocato dello studio Previti

Gran parte delle aziende non ha ancora piena consapevolezza che la compliance e quindi anche le questioni della privacy e della sicurezza informatica sono parte integrante del business

Giuseppe Di Masi
Partner dello studio Sza

Sui flussi di dati Usa-Ue mancano ancora i contenuti del nuovo accordo. Nel frattempo si continua a navigare a vista, considerato che oggi tutti i nostri principali strumenti digitali sono made in Usa

Alessandro Vercellotti
Fondatore dello studio Legal For Digital