Primo Piano
Tecnologia e imprese

Privacy Shield

Regole inadeguate
Il Privacy Shield, l'accordo bilaterale Ue-Usa sulla privacy approvato nel 2016 dalla Commissione Ue, è stato invalidato dalla Corte di Giustizia europea nel 2020 (sentenza Schrems II). La Corte ha ritenuto inadeguate le misure di sicurezza previste dagli Stati Uniti per tutelare i dati. Ancora oggi le società americane sono in difficoltà nell'attivare misure in linea con la nuova disciplina: un problema per i player europei che "esportano" dati personali negli Usa.

Contratti a distanza: senza lo scudo privacy a rischio i dati aziendali

Firme digitali. Complice la pandemia, cresce l'uso della contract automation
Ma resta il nodo del trattamento dei documenti da parte dei provider extra Ue

Dario Aquaro
Alessandro Longo

La prossima big tech sarà una "legal tech", anche se non si chiamerà così. La battuta corre tra ingegneri e avvocati d'affari e fotografa bene una realtà: quella dei dati societari e del loro valore. Una realtà rappresentata dai contratti a distanza firmati in digitale tra aziende.

Mercato e analisi dei dati

Il settore della *contract automation* è in veloce espansione, complici gli sviluppi tecnologici e la pandemia. Ma è dominato da pochi grandi player. I principali attori dell'*e-signature* – secondo uno studio Idc del settembre scorso – sono Docusign (oltre un milione di clienti e un miliardo di utenti), Adobesign e Infocert, tallonati da Hellosign (che può contare sugli oltre 16 milioni di utenti paganti di Dropbox) e Namirial. Mentre anche Google ha investito in questo mercato, siglando una partnership con IronClad.
«Spesso le aziende – spiega Carlo Rossi Chauvenet, partner dello studio legale CrcLex – si pongono dubbi solo sulla validità del contratto, che dipende dal fornitore del servizio e dalla tipologia di firma elettronica scelta (semplice, avanzata o qualificata, a seconda dei casi). Si sottovaluta però il problema del controllo sull'uso dei dati raccolti dai documenti sottoscritti, considerato che queste società di software godono anche di un effetto network, amplificativo: più i loro servizi sono usati, più si diffondono».

«Molte grandi aziende europee, ad esempio, hanno addirittura introdotto una "clausola Docusign" nei modelli di contratto con i fornitori, inducendoli a usare questa piattaforma per siglare a distanza e ad usarla a cascata con propri i subfornitori. La questione – sintetizza Rossi Chauvenet – riguarda, da un lato, la capacità di alcuni soggetti di tenere in mano il mercato della *contract automation*, accumulando enormi quantità di dati sensibili in server all'estero. E dall'altro la capacità di leggere questi dati a fini statistici, grazie ai sistemi evoluti di *analytics*, alla leva dell'intelligenza artificiale. In sostanza, trasferiamo dati aziendali riservati che, presto o tardi, potrebbero essere usati per monitorare i flussi economici e i mercati in tempo reale» (si veda l'altro articolo).

Tra business e privacy

Anche i *provider* Usa come Docusign, che dichiara di controllare circa il 70% del mercato delle firme elettroniche, hanno sedi europee, per cui i trattamenti di dati dei clienti connessi alla fornitura dei servizi sono "nativamente" soggetti al Gdpr. «Ma la protezione scatta su dati che identificano o rendono identificabile una persona fisica, e ne sono esclusi – oltre ai dati delle persone giuridiche – anche quelli anonimi o anonimizzati», osserva l'avvocato Alessandro Del Ninno, docente e partner dello studio legale Tonucci & Partners. Che precisa: «Da questo punto di vista, anche l'eventuale aggregazione dei dati non è una misura sufficiente a escludere l'applicabilità della normativa *data protection*: molto spesso le aziende credono che sia sufficiente aggregare i dati per renderli anonimi, mentre essi possono rimanere in tutto e per tutto "personali", se si può risalire dall'aggregazione all'identificazione delle persone fisiche a cui i dati aggregati si riferiscono, attraverso una sorta di "*data reverse engineering*". In questi casi resta dunque applicabile il Gdpr. Senza contare che molte società dichiarano di conservare i "*transaction data*" per tutto il tempo necessario alle proprie finalità commerciali».

I rapporti con gli Usa

I legali che assistono le aziende prendono ovviamente in esame tutti i termini contrattuali. Ma sui dati non personali (anonimi) – e utilizzabili a fine statistico per "mappare" le relazioni tra imprese – non c'è una normativa specifica. «Occorre muoversi tra più riferimenti», nota Giulio Novellini, counsel dello studio Portolano Cavallo. E quindi: il regolamento 1807/2018 sulla libera circolazione dei dati non personali nella Ue, che prevede di rispettare principi in parte simili a quelli del Gdpr, come la portabilità del dato, soprattutto nei rapporti di *outsourcing*; il Dlgs 133/2019 sulla cyber sicurezza, per difendere i dati e gestire i casi di *data breach*; e il prossimo regolamento Ue (ora in bozza) sugli usi dell'intelligenza artificiale.

Quanto al trasferimento dati tra Paesi Ue e Stati Uniti, c'è però un problema di *data protection* sollevato dalla sentenza Schrems II (del 16 luglio 2020). «La Corte di Giustizia Ue – dice Novellini – ha infatti ritenuto inadeguato l'accordo bilaterale (*privacy shield*), inadeguate le misure di sicurezza previste dagli Usa per tutelare i dati. Ancora oggi le società americane sono in difficoltà nell'implementare misure in linea con la nuova disciplina: per i player europei che "esportano" dati personali negli Usa risulta perciò difficile provare che la loro struttura tecnico-organizzativa sia all'altezza. È un problema aperto, al momento c'è poca giurisprudenza, solo qualche interpretazione da parte di alcune Autorità privacy europee. E vale per i dati personali, ma potrebbe estendersi anche a quelli societari».

Asset strategici

Il valore di questi dati, spiegano gli esperti, aiuta a capire quanto possa essere importante trasformare la burocrazia in asset. E sviluppare un forte player europeo. Il principale attore continentale è italiano: Infocert, che opera in venti Paesi e – come racconta Carmine Auletta, Chief innovation & strategy officer – «dal 2016 ha cavalcato la discontinuità normativa che è arrivata con il regolamento europeo Eidas sull'identità digitale» (che disciplina tra l'altro le firme elettroniche, *ndr*).

Infocert si è quindi fatta strada appagando un bisogno crescente di molte aziende che usano la contrattualistica a distanza: le rassicurazioni sui dati e la bontà della firma. «Adobe e Docusign operano come fornitori di software e pongono tutte le responsabilità sulla validità della firma in capo all'utente. Noi siamo accreditati in Europa come fornitori di servizi qualificati: un attore che si prende responsabilità sulla validità della firma e l'identità del soggetto firmatario, e che garantisce la residenza del dato in Europa», rimarca Auletta. Con una postilla: «In Francia e Germania, più che in Italia, ci sono aziende più sensibili al tema della possibilità di accesso ai dati da parte dell'intelligence americana».

> **Manca una normativa specifica sulla protezione dei dati non personali, che possono essere letti a fine statistico**

STEFANO MARRA

Contratto in cinque mosse

I PASSAGGI
Dalla proposta di accordo (con firma qualificata) fino all'archiviazione

1. **L'impresa A mette a punto un documento contrattuale e lo carica nell'applicativo**
2. **L'impresa A firma elettronicamente il contratto e invia (tramite mail) una richiesta all'impresa B**
3. **L'impresa B visualizza il documento all'interno dell'applicazione e lo verifica**
4. **L'impresa B appone la firma elettronica e convalidala propria identità tramite un codice univoco**
5. **Il file può essere archiviato in cloud e conservato per un certo periodo**

Quando il documento viene firmato nell'applicativo, l'impresa A riceve una notifica dell'avvenuta approvazione

DIVERSI TIPI DI E-SIGNATURE
Il livello di tutela e sicurezza della firma elettronica dipende dalla tipologia scelta: semplice, avanzata o qualificata.

SEMPLICE
La firma elettronica semplice è la più "debole": un mero strumento di sottoscrizione (ad esempio, il login tramite username e password)

AVANZATA
La firma elettronica avanzata presuppone la previa identificazione del firmatario (ad esempio, la firma grafometrica, tramite pennino su tablet). Ha la valenza probatoria della scrittura privata

QUALIFICATA
La firma elettronica qualificata si basa sul certificato di un ente garante dell'autenticità, e viene creata tramite dispositivi elettronici (smart card, chiavette Usb, token). Equivale a una firma autografa

DIGITALE
La firma digitale è la forma più evoluta di firma elettronica qualificata: si aggiunge la conferma tramite Pin

Così l'intelligenza artificiale può scardinare l'anonimato

Analisi e profilazioni

Gli algoritmi sono in grado di rivelare accordi, attività e investimenti societari

«In internet nessuno sa se sei un cane», dicevano due cani in una famosa vignetta diffusa agli albori della rete. Adesso è tutto il contrario: è possibile scoprire chi siamo, e altre nostre caratteristiche, anche se i dati di partenza sono all'apparenza anonimi. Il motivo è duplice: utilizzo di algoritmi di intelligenza artificiale in grado di elaborare quei dati e accumulo di *big data*, ossia grandi masse di informazioni che è possibile incrociare.

Anche nel caso dei servizi di *contract automation* «c'è un rischio di re-identificare i soggetti che stipulano un contratto, anche se in teoria questi dati sono stati resi anonimi», afferma Guido Scorza, del collegio del Garante Privacy. «Ad esempio – dice – se un'azienda si trova a firmare più contratti indicando uno stesso domicilio o un Cap dove ci sono poche utenze, è facilmente identificabile dagli algoritmi di analisi. Algoritmi che, mettendo assieme i diversi dati, potrebbero rivelare contratti, investimenti e attività aziendali». Il rischio è più elevato quanto più concentrato è il mercato del *provider*, perché i dati (contrattuali in questo caso) vengono ammassati in poche mani. «Un discorso che vale per qualsiasi fornitore di servizi *cloud*», aggiunge Scorza.

Gli impatti sono di privacy – per persone fisiche, collaboratori, clienti o fornitori dell'azienda citati nel contratto – ma anche di tipo economico e geopolitico. Il gestore del servizio può infatti accumulare informazioni strategiche rilevanti su interi comparti economici. E in teoria può farlo anche il suo Governo, nei Paesi dove le aziende sono tenute ad aprire queste informazioni alle autorità.

Il rischio di re-identificazione su dati "anonimi" tramite intelligenza artificiale è stato del resto provato da molti studi. In uno del 2019, ad esempio, 1 ricercatori delle Università di Londra e di Lovanio (Belgio) sono riusciti a re-identificare alcuni politici e giuristi analizzando la cronologia web "anonima" di tre milioni di cittadini tedeschi, mostrando di saper svelare dati relativi alla salute o alle preferenze sessuali.

Il problema è noto da tempo, e già nel 2006 due ricercatori dell'Università del Texas erano riusciti a identificare mezzo milione di utenti Netflix. Con gli anni sono arrivate diverse tecniche più robuste di (pseudo) anonimizzazione, ma una soluzione definitiva ancora non c'è; anche perché maturano in parallelo le tecniche per re-identificare e profilare gli utenti.

Il nodo dei dati all'estero

L'attuale normativa Ue sulla privacy prova a stabilire alcune tutele generali. «Il Gdpr è stato elaborato proprio per regolare anche questi fenomeni e dare agli interessati un controllo adeguato sui loro dati anche nell'epoca digitale», commenta Franco Pizzetti, ex Garante privacy, professore di Diritto costituzionale all'Università di Torino. Insomma: consapevoli che la tecnologia (intelligenza artificiale ma non solo) potrà sempre permettere qualsiasi tipo di abuso sui nostri dati, la sola salvezza è costruire un sistema che dia garanzie e fiducia; tali per cui gli esiti peggiori, sebbene tecnicamente possibili, non avvengano.

Questo paradigma entra in crisi con il trasferimento dei dati all'estero. Pizzetti spiega che «l'Europa ragiona così: se la legislazione del Paese di destinazione non assicura analoghe garanzie, gli interessati non possono avere fiducia nei trattamenti dei dati; ecco perché la normativa europea vieta i trasferimenti». Ma non solo: «Proprio perché il possesso dei dati consente la loro analisi e di trarre da essi nuove informazioni, è evidente che trasferire dati all'estero, e in particolare a chi li tratta fuori dall'Unione, significa "donare il sangue" (cioè i dati) a terzi, consentendo di trarre altre informazioni sulla Ue, la sua economia, la sua civiltà e le relazioni dei suoi operatori a livello globale».

> **Come per i fornitori di servizi cloud, il rischio di violazioni è più elevato se il mercato si concentra nelle mani di pochi**

È proprio negli Usa che si trovano i maggiori fornitori di servizi *cloud* e le più diffuse tecnologie di intelligenza artificiale. Come spiega ancora Pizzetti, siamo in una fase di fragile equilibrio, in cui «tutto si regge su accordi contrattuali che i fornitori dei servizi operanti negli Usa devono dare a chi si avvale dei loro servizi e questi ultimi devono dare ai loro utenti circa la tutela e la difesa delle informazioni. Una pura foglia di fico, neanche molto elegante, per non bloccare tutto».

Non è chiaro quale soluzione troveranno Ue e Stati Uniti per garantire ai "cani anonimi" della vignetta di restare tali; anche nell'era dell'intelligenza artificiale e dei *big data*, e anche nella necessità di fare circolare dati e servizi. Secondo alcuni la soluzione non può venire solo dalle norme: «La debolezza industriale Ue non consente grandi spazi di manovra. Per questo motivo – chiosa Pizzetti – è così importante la corsa della Ue, con il Pnrr, a uno sviluppo adeguato delle tecnologie digitali».

—**Al. Lo.**