DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

Trump V. Slaughter: i riflessi nel Data Privacy Framework UE-USA

In che termini il rischio istituzionale entra nei contratti con i fornitori americani

22 Luglio 2026

Alessandro Ferrari, Partner, Head of Technology Sector, DLA Piper

Alessandro Ferrari, Partner, Head of Technology Sector, DLA Piper

Alessandro Ferrari

Alessandro Ferrari è Partner del dipartimento Intellectual Property & Technology e dirige il Sector Technology in Italia e si occupa principalmente di diritto applicato alla tecnologia, assistendo i clienti in questioni transactional, advisory and IT litigation. Ha esperienza nella redazione e negoziazione di accordi strategici e cross-border di outsourcing di processi aziendali e di altri contratti commerciali, IT e relativi alla proprietà intellettuale in diversi settori e in diverse geografie. Ha inoltre esperienza nella consulenza su tutti gli aspetti del processo di sourcing/approvvigionamento, compreso lo sviluppo della struttura dell'accordo, la negoziazione e l'assistenza ai clienti nell'implementazione e nelle strategie di integrazione, nella governance e nei performance management regimes.

Studio Legale Tributario Associato

DLA Piper

Una sentenza americana sulla separazione dei poteri può sembrare lontana dai contratti cloud di una istituzione finanziaria europea. Trump v. Slaughter dimostra il contrario.

Il 29 giugno 2026 la Supreme Court degli Stati Uniti ha riconosciuto il potere del Presidente di rimuovere Rebecca Slaughter, commissioner della Federal Trade Commission, superando il precedente Humphrey's Executor del 1935. Quel precedente aveva per decenni consentito al Congresso di proteggere i commissari di alcune agenzie indipendenti dalla rimozione presidenziale "at will". La Corte ha invece ritenuto che, nella configurazione attuale della FTC, le protezioni statutarie alla rimozione siano incompatibili con la separazione dei poteri.

La decisione non riguarda direttamente il GDPR e non contiene alcuna valutazione sul Data Privacy Framework UE-USA. Eppure, il suo effetto potenziale arriva su uno dei profili che più interessano il diritto europeo dei trasferimenti: la credibilità istituzionale delle garanzie offerte dal Paese terzo.

Il Data Privacy Framework si regge sugli impegni delle società americane e sulla possibilità che quegli impegni siano verificabili, azionabili e presidiati da autorità capaci di intervenire. Le imprese statunitensi che aderiscono al DPF si autocertificano presso il Department of Commerce, ma la mancata conformità ai principi del framework può integrare una pratica scorretta o ingannevole ai sensi della Section 5 del FTC Act, aprendo la strada all'intervento della FTC.

È qui che Trump v. Slaughter diventa rilevante per l'Europa. Se l'autorità chiamata a far rispettare una parte essenziale degli impegni DPF vede ridimensionata la propria indipendenza dal potere esecutivo, la domanda diventa inevitabile: il sistema continua a offrire un livello di protezione sostanzialmente equivalente a quello garantito nell'Unione?

Occorre essere precisi. Il DPF resta valido. La decisione di adeguatezza della Commissione europea del 10 luglio 2023 non è stata ritirata dalla Commissione né annullata dalla Corte di giustizia. Le società certificate possono continuare a ricevere dati personali dall'UE sulla base del framework, nei limiti in cui la certificazione sia effettiva e il trasferimento rientri nel suo ambito. Trump v. Slaughter non produce un effetto automatico di invalidazione.

Il quadro era stato peraltro confermato dal Tribunale dell'Unione europea nel caso Latombe, con una

vedi l'articolo online

valutazione riferita alla situazione esistente al momento dell'adozione della decisione di adeguatezza. Proprio per questo, un cambiamento successivo dell'assetto istituzionale americano può diventare rilevante nei futuri monitoraggi o contenziosi.

Sarebbe però poco prudente liquidare la vicenda come un tema accademico di diritto costituzionale americano. La storia dei trasferimenti UE-USA mostra che la tenuta dei meccanismi di adeguatezza dipende anche da elementi istituzionali: indipendenza dei controlli, effettività dei rimedi, possibilità per l'interessato di ottenere tutela, limiti all'accesso pubblico ai dati e capacità delle autorità di enforcement di agire in modo credibile.

Safe Harbour e Privacy Shield sono caduti davanti alla Corte di giustizia perché il sistema, secondo la Corte, non assicurava garanzie essenzialmente equivalenti a quelle europee rispetto all'accesso delle autorità pubbliche e ai rimedi disponibili per gli interessati. Il DPF nasce per rispondere a quelle criticità, attraverso un pacchetto di nuove salvaguardie, tra cui l'Executive Order 14086, il Data Protection Review Court e una rinnovata architettura di compliance per le società certificate.

La sentenza della Supreme Court non interviene su tutti questi elementi allo stesso modo. La questione FTC riguarda soprattutto la dimensione commerciale del DPF: l'adesione delle società ai principi, la correttezza delle dichiarazioni rese, il rispetto degli obblighi verso gli interessati e l'enforcement in caso di violazioni. Resta distinto, pur collegato nel giudizio complessivo di adeguatezza, il tema dell'accesso ai dati da parte delle autorità di intelligence e dei rimedi previsti per tale accesso.

Questa distinzione è utile anche per le imprese. Lo scenario da evitare è scoprire troppo tardi che alcuni flussi critici dipendono esclusivamente dal DPF, senza un piano contrattuale e organizzativo già pronto nel caso in cui il framework sia modificato, sospeso, contestato con successo o oggetto di nuove indicazioni da parte della Commissione, dell'EDPB o delle autorità nazionali.

NOYB ha già collegato espressamente Trump v. Slaughter alla tenuta dei trasferimenti UE-USA, chiedendo alla Commissione europea di ritirare la decisione di adeguatezza. Secondo NOYB, l'indipendenza della FTC era un elemento su cui la Commissione aveva fatto affidamento nell'impianto del DPF. È una posizione di parte, ma non marginale: Schrems I e Schrems II hanno già ridisegnato per due volte l'infrastruttura giuridica dei trasferimenti transatlantici.

Dal punto di vista di banche, assicurazioni e intermediari finanziari, il tema va letto dentro una cornice più ampia. I trasferimenti internazionali sono spesso una componente strutturale di servizi cloud, outsourcing ICT, soluzioni antifrode, CRM, marketing automation, piattaforme HR, sistemi di collaborazione, cybersecurity monitoring, data analytics e strumenti di intelligenza artificiale. In molti casi, il dato non "parte" verso gli Stati Uniti in modo visibile al business owner. Può farlo tramite supporto tecnico, log, subfornitori, data lake, funzioni di model improvement, incident response, remote administration o accessi da team globali.

L'esperienza sui contratti tecnologici e sull'outsourcing per operatori regolati insegna sovente che il rischio nasce spesso da una separazione artificiale tra negoziazione commerciale, data protection e vendor governance. Il procurement guarda al servizio, il legal guarda al contratto, il privacy team guarda al DPA, l'ICT guarda all'architettura e il risk team guarda alla criticità del fornitore. Quando il trasferimento internazionale viene trattato come mero "allegato privacy", si perde il collegamento con continuità operativa, exit, sub-outsourcing, audit, sicurezza, localizzazione dei dati e capacità effettiva di sostituire un provider.

Trump v. Slaughter è un promemoria di questo collegamento. Il DPF dovrebbe essere gestito nel ciclo di vita del rapporto con il fornitore. La questione operativa è se l'impresa sia in grado di continuare il servizio, documentare la compliance e gestire il contratto qualora il DPF diventasse meno stabile.

La prima verifica è la mappatura. Le imprese dovrebbero sapere quali fornitori statunitensi ricevono dati personali sulla base del DPF, quali dati ricevono, per quali finalità, attraverso quali sistemi e con quali subfornitori. Questa ricognizione dovrebbe includere i grandi cloud provider e le piattaforme SaaS più rilevanti, ma anche ticketing, customer engagement, vulnerability management, threat intelligence, AI API, analytics e supporto tecnico.

La seconda verifica riguarda il contratto. In diversi accordi si trova una formula apparentemente rassicurante: il fornitore dichiara di essere certificato DPF e si impegna a mantenere la certificazione. È utile, ma spesso non risolve il problema operativo. Occorre capire cosa accade se la certificazione viene meno, se il fornitore esce dalla Data Privacy Framework List, se la Commissione modifica o sospende la decisione di adeguatezza, se un'autorità europea contesta determinati trasferimenti o se il framework

vedi l'articolo online

viene sottoposto a una nuova challenge giudiziaria.

In un DPA ben costruito, questi scenari dovrebbero attivare obblighi precisi: notifica tempestiva, cooperazione, messa a disposizione delle informazioni necessarie per valutare il trasferimento, disponibilità a sottoscrivere SCC aggiornate, supporto al transfer impact assessment, implementazione di misure supplementari, revisione dei subprocessor e, nei casi più delicati, possibilità di riorganizzare il servizio o limitare determinate categorie di accesso.

La terza verifica riguarda SCC e transfer impact assessment. Molte imprese hanno mantenuto, accanto al DPF, una fallback contrattuale sulle clausole tipo. È una scelta prudente, purché sia effettiva. Le SCC non sono un paracadute se restano in un allegato non aggiornato, non coordinato con il DPA e non supportato da un'analisi documentata del contesto di trasferimento. Dopo Schrems II, l'EDPB ha chiarito che l'esportatore deve conoscere i propri trasferimenti, valutare il diritto e la prassi del Paese terzo e adottare misure supplementari quando necessario. Questa logica diventa il piano di continuità regolatoria se la decisione di adeguatezza viene messa sotto pressione.

Anche le misure tecniche e organizzative meritano una verifica reale. Nei trasferimenti verso gli Stati Uniti, le misure supplementari non possono essere descritte in modo generico. Per alcune architetture, cifratura con chiavi in Europa, pseudonimizzazione, segregazione dei dati, minimizzazione dei log, limitazione degli accessi amministrativi o regionalizzazione effettiva possono fare la differenza. Per altre architetture, soprattutto quando il provider deve accedere ai dati in chiaro per erogare il servizio, serve una valutazione più accurata del rischio residuo.

Un ulteriore profilo riguarda la governance del cambiamento. I servizi digitali cambiano continuamente. Un provider cloud introduce nuove region, una piattaforma AI modifica le funzioni di training, un servizio cybersecurity attiva un nuovo subprocessor, una suite SaaS sposta attività di supporto. Se il contratto non collega questi cambiamenti a un obbligo di valutazione preventiva dei trasferimenti, il presidio privacy resta arretrato rispetto all'evoluzione tecnica del servizio.

Per gli operatori vigilati, questo ragionamento incontra anche DORA e le regole sull'ICT third-party risk. Un fornitore cloud o SaaS che supporta funzioni importanti o critiche non è soltanto un processor GDPR. È parte dell'architettura di resilienza operativa dell'impresa. La fragilità del meccanismo di trasferimento può diventare un rischio di continuità, un tema di exit strategy, una questione di concentrazione e un elemento della due diligence sul sub-outsourcing.

La posizione più equilibrata, oggi, è intermedia. Non c'è ragione per creare allarme. C'è però una ragione concreta per rivedere le dipendenze regolatorie dai trasferimenti UE-USA, soprattutto nei contratti nuovi o in fase di rinnovo. Ogni nuova negoziazione cloud, SaaS, AI o cybersecurity con un provider statunitense dovrebbe includere una domanda esplicita: se domani il DPF non fosse più sufficiente, il contratto e l'architettura operativa sarebbero in grado di reggere?

Serve sapere se il provider accetta trigger di revisione, se consente misure tecniche aggiuntive, se offre alternative di localizzazione, se permette la disattivazione di determinati flussi, se collabora nella TIA e se gli obblighi sui subfornitori sono abbastanza granulari.

Per le imprese già esposte, una due diligence mirata può essere più efficace di una revisione generalizzata. I criteri di priorità sono abbastanza chiari: criticità del servizio, volume e natura dei dati, presenza di dati particolari o dati finanziari sensibili, ruolo del fornitore nella catena operativa, impossibilità di sostituzione rapida, dipendenza da subprocessor statunitensi, accesso ai dati in chiaro, uso di AI o analytics, e rilevanza del servizio per continuità operativa o controlli di sicurezza.

Per le nuove negoziazioni, invece, il tema andrebbe incorporato fin dall'inizio nella strategia contrattuale. Nei contratti più maturi, la clausola sui trasferimenti funziona come una clausola di gestione del rischio regolatorio: individua basi alternative, disciplina i cambiamenti del framework, impone obblighi di cooperazione, consente la revisione delle misure, coordina DPA, SCC, subprocessing, audit, sicurezza, business continuity ed exit.

È probabile che Trump v. Slaughter non sia l'ultima parola sul DPF. La Commissione potrà valutare se e come considerare l'evoluzione della giurisprudenza americana nei prossimi monitoraggi. Le autorità europee potranno intervenire con orientamenti o prese di posizione. Le challenge promosse da attivisti o operatori potranno portare il tema davanti ai giudici europei. Nel frattempo, il framework resta operativo.

Proprio per questo il momento per intervenire è adesso. Quando una decisione di adeguatezza viene

annullata, la compliance diventa emergenza. Quando mostra segnali di fragilità, può ancora essere gestita come governance contrattuale.

La lezione pratica di Trump v. Slaughter è trattare il DPF come una dipendenza regolatoria da monitorare e contrattualizzare. Per gli operatori regolati e per le imprese con catene tecnologiche complesse, questa differenza è decisiva: trasforma un rischio giuridico futuro in una decisione di procurement di oggi.

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it