Analisi · 18 maggio 2026

← Precedente·Successivo →

Schrems II, cinque anni dopo

La sentenza che ha cambiato il diritto dei trasferimenti internazionali di dati personali. Cinque anni dopo, una parte considerevole dell'attività quotidiana degli uffici europei continua a operare come se nulla fosse accaduto.

La sentenza che ha impiegato tre ore per cambiare le regole

Il 16 luglio 2020, verso le dieci e un quarto del mattino, ora di Lussemburgo, la Corte di Giustizia dell'Unione Europea ha reso nota la sentenza nella causa C-311/18. Nelle tre ore successive, il regime giuridico che sosteneva il trasferimento quotidiano di dati personali dall'Europa agli Stati Uniti —il cosiddetto Scudo per la privacy, Privacy Shield nella sua denominazione ufficiale— ha cessato di esistere. Quando i responsabili della protezione dei dati europei hanno finito di pranzare quel giorno, il quadro entro cui operavano le loro aziende e amministrazioni non era più valido.

La sentenza è nota oggi come Schrems II, dal nome di Maximilian Schrems, l'attivista austriaco la cui denuncia contro Facebook Ireland l'ha innescata. La denuncia, nello specifico, riguardava i trasferimenti tra Facebook Irlanda e Facebook Stati Uniti. La sentenza, in generale, va molto oltre: stabilisce come e a quali condizioni qualsiasi dato personale raccolto in territorio europeo possa essere trasferito negli Stati Uniti.

Quasi sei anni dopo, esiste il quadro sostitutivo —l'EU-US Data Privacy Framework, adottato a luglio 2023— ed è anch'esso sotto pressione giuridica. Si prepara un nuovo round Schrems. Nel frattempo, le piccole e medie imprese europee continuano a utilizzare servizi cloud statunitensi per le attività quotidiane, per lo più ignorando che la questione giuridica su cui si basano tali servizi rimane aperta.

Cosa diceva esattamente Schrems II

La sentenza si fonda su tre pilastri. Il primo è la Carta dei diritti fondamentali dell'Unione Europea, in particolare gli articoli 7 (vita privata e familiare), 8 (protezione dei dati personali) e 47 (tutela giurisdizionale effettiva). Il secondo è il Regolamento generale sulla protezione dei dati —il GDPR che molti europei ricordano solo per gli avvisi sui cookie—, specificamente il Capo V, articoli da 44 a 50, sui trasferimenti internazionali. Il terzo è la legislazione statunitense in materia di intelligence: la sezione 702 del Foreign Intelligence Surveillance Act, FISA 702 in gergo legale, e l'Ordine Esecutivo presidenziale 12333.

La Corte ha proceduto per contrasto. La Carta dei diritti fondamentali esige che i dati personali dei cittadini europei godano, quando lasciano l'Unione, di un livello di protezione essenzialmente equivalente a quello garantito dal GDPR. La domanda era, di conseguenza, se gli Stati Uniti offrissero tale livello essenzialmente equivalente.

La risposta è stata negativa, e non per sfumature. La sezione 702 della FISA consente al governo statunitense di raccogliere comunicazioni di non statunitensi situati al di fuori del territorio nazionale senza previa autorizzazione giudiziaria individuale, senza notifica all'interessato e senza un ricorso effettivo paragonabile a quello europeo. L'Ordine Esecutivo 12333 estende tale capacità in modo analogo al di fuori del territorio nazionale. La Corte ha concluso che il cittadino europeo, di fronte al sistema giuridico statunitense, non dispone della protezione essenzialmente equivalente richiesta dalla Carta. L'equivalenza, pertanto, non esiste.

Da qui la conseguenza diretta: la Decisione 2016/1250 della Commissione Europea, che aveva validato il Privacy Shield come quadro adeguato per i trasferimenti, è stata dichiarata invalida. Ogni trasferimento basato esclusivamente su tale quadro è rimasto privo di base giuridica da quel preciso istante.

Cosa è sopravvissuto (e a quali condizioni)

Schrems II non ha eliminato tutti gli strumenti. Le Clausole Contrattuali Tipo —gli SCC nel gergo internazionale, dall'inglese Standard Contractual Clauses— sono sopravvissute. Si tratta di contratti tipo approvati dalla Commissione Europea: un esportatore europeo e un importatore del paese di destinazione li firmano impegnandosi a trattare i dati secondo lo standard europeo. L'azienda che pensava di aver risolto il problema il 17 luglio 2020 ha firmato le SCC con il proprio fornitore e si è ritenuta soddisfatta.

L'inquietudine è arrivata leggendo la sentenza con attenzione. La Corte ha chiarito che le SCC rimangono valide, ma la loro validità dipende da una condizione che conviene sottolineare: che l'importatore dei dati possa rispettarle nella pratica. Se la legislazione nazionale del paese di destinazione gli impedisce di rispettare le clausole —perché, ad esempio, un ordine ai sensi della FISA 702 lo obbliga a consegnare i dati senza informare la controparte europea—, le clausole non proteggono realmente. In tal caso, afferma la Corte, l'esportatore europeo deve sospendere il trasferimento.

Ciò ha introdotto un nuovo elemento nella pratica europea della protezione dei dati: la Transfer Impact Assessment, o analisi dell'impatto del trasferimento, nota con l'acronimo TIA. Ogni volta che un'azienda europea vuole trasferire dati negli Stati Uniti sulla base delle SCC, deve valutare formalmente se il destinatario possa rispettare le clausole data la legislazione ad esso applicabile. Il Comitato europeo per la protezione dei dati (EDPB) ha pubblicato orientamenti dettagliati su come condurre la TIA. La pratica onesta porta solitamente allo stesso risultato: se l'importatore è una filiale statunitense di un colosso del cloud, la risposta sincera alla TIA è che le clausole non possono essere rispettate così come sono scritte.

Il Privacy Framework e lo Schrems III pendente

Il 10 luglio 2023, la Commissione Europea ha adottato una nuova Decisione di Adeguatezza: la 2023/1795. Sostituisce il defunto Privacy Shield e opera sotto il nome di EU-US Data Privacy Framework. Gli Stati Uniti avevano precedentemente modificato il proprio regime interno tramite l'Ordine Esecutivo 14086, che limita la portata dell'intelligence dei segnali a quanto «necessario e proporzionato» —terminologia familiare per il lettore europeo, meno per la pratica amministrativa statunitense— e crea un organo di revisione chiamato Data Protection Review Court (DPRC). La Commissione ha ritenuto che tali modifiche fossero sufficienti per ripristinare il livello essenzialmente equivalente.

L'organizzazione noyb, fondata da Schrems, ha presentato una denuncia il 7 settembre 2023 contro la nuova Decisione. Gli argomenti sono quelli prevedibili: il DPRC non è un tribunale indipendente ai sensi dell'Articolo 47 della Carta; i concetti di «necessario e proporzionato» non traducono meccanicamente gli standard europei; e, infine, una protezione basata su un Ordine Esecutivo può essere revocata dall'Ordine Esecutivo successivo. Una sentenza della CGUE sulla nuova Decisione —quella che molti chiamano già, con una certa rassegnazione, Schrems III— è attesa per i prossimi anni. L'esito non può essere anticipato. La struttura dell'argomentazione, in ogni caso, ricorda molto quella del 2020.

Quello che la PMI europea non sente

Mentre la Grande Sezione della CGUE delibera, lo studio legale di medie dimensioni continua a scambiarsi corrispondenza con i propri clienti tramite Microsoft 365, ospitato in regioni europee ma di proprietà di un'azienda statunitense soggetta alla FISA 702. Lo studio medico privato sincronizza le agende tramite Google Workspace. Il consulente fiscale invia dichiarazioni firmate tramite DocuSign. Lo psicologo fattura da un foglio di calcolo in Notion. Lo studio giuslavorista archivia i fascicoli in Dropbox. E praticamente tutti, inoltre,

assistono i propri clienti su WhatsApp. Tutto ciò può operare, secondo i fornitori, sulla base della Decisione di Adeguatezza 2023/1795. Il giorno in cui tale Decisione cadrà con Schrems III, tutti questi rapporti rimarranno scoperti nello stesso istante.

La questione non è retorica. Tra il 2022 e il 2024, diverse autorità europee hanno risolto procedimenti contro titolari del trattamento per l'utilizzo di Google Analytics senza un adeguato strumento di trasferimento, applicando letteralmente il ragionamento della CGUE ancor prima dell'entrata in vigore del Privacy Framework. L'autorità francese, la CNIL, è stata la prima a formalizzare il criterio nel 2022; le autorità austriaca, italiana e altre hanno seguito poco dopo. L'inadempienza, nell'attuale assetto operativo della PMI europea, è documentata in tempo reale per chiunque sappia dove guardare.

La TIA come strumento, non come rituale

Una parte considerevole delle TIA che circolano negli uffici europei sono, a ben guardare, esercizi formali. Elencano gli strumenti contrattuali, enumerano le certificazioni del fornitore, citano le garanzie tecniche, spuntano la casella. Poche si chiedono seriamente se un ordine FISA 702 obbligherebbe il fornitore a consegnare i dati. Ancora meno si chiedono cosa accadrebbe a quel trasferimento in caso di ipotetica revisione del Privacy Framework. L'Articolo 5 del GDPR impone al titolare del trattamento di essere in grado di dimostrare la conformità. Una TIA che non viene eseguita seriamente non dimostra nulla; ciò che dimostra è la volontà di conformarsi sulla carta mentre si fa l'opposto nella pratica.

La versione sincera della TIA inizia con una domanda semplice: cosa accadrebbe se domani arrivasse a questo fornitore un ordine FISA 702 riguardante questi dati specifici? Se la risposta onesta è «dovrebbe consegnarli senza avvisarci», le clausole contrattuali non risolvono il problema. Ciò che lo risolve, nei casi in cui la domanda conta davvero, è non aver messo il dato nelle mani di quel fornitore.

Il cambiamento politico come rischio strutturale

C'è un ulteriore strato, politico, che conviene nominare senza drammi. La Decisione di Adeguatezza 2023/1795 poggia, in ultima analisi, sull'Ordine Esecutivo 14086, firmato dal presidente Biden nell'ottobre 2022. Un Ordine Esecutivo viene firmato da un presidente e può essere revocato, modificato o svuotato di contenuto dal successivo. La protezione dei dati europei negli Stati Uniti dipende, così, da una decisione amministrativa che né il Congresso americano garantisce né il sistema giuridico americano protegge con la solidità con cui protegge altre materie interne. Da gennaio 2025 una nuova amministrazione guida gli Stati Uniti, e la questione sulla continuità pratica dell'EO 14086 è passata dall'essere un'ipotesi a diventare realtà contemporanea. Qualsiasi scenario in cui l'amministrazione decida di ritirare o attenuare l'Ordine lascerebbe la Decisione Europea priva del pezzo su cui è stata costruita.

Non è un argomento cospirativo. È la lettura sobria del disegno giuridico. I quadri di protezione dei dati transatlantici sono già caduti due volte: il Safe Harbor nel 2015 (sentenza Schrems I), il Privacy Shield nel 2020 (Schrems II). Il terzo poggia su un elemento più fragile dei suoi due predecessori. Un'azienda europea che scommette oggi il proprio trattamento dei dati su quel pezzo sta prendendo una decisione di gestione del rischio, non di mera conformità normativa.

Per il lettore professionista

Le domande operative che conviene porsi prima di scegliere un servizio cloud per dati professionali —con il rigor con cui le porrebbe un ispettore della protezione dei dati— sono le seguenti:

1. Dove sono conservati fisicamente i dati? Una regione europea non è una risposta sufficiente se l'operatore è statunitense.
2. Chi gestisce il servizio, in quale giurisdizione è costituito e a quali ordini legali può essere sottoposto?

3. Quale strumento di trasferimento viene invocato: Decisione di Adeguatezza 2023/1795, SCC con TIA, deroga dell'Articolo 49 del GDPR? Questa scelta è difendibile in caso di ispezione?
4. Se la Decisione di Adeguatezza dovesse cadere domani, quale piano operativo esiste per mantenere l'attività?
5. Esiste un'alternativa europea o self-hosted per tale funzione e quale sarebbe il costo reale della migrazione?

Non tutte le funzioni dell'ufficio quotidiano richiedono la stessa risposta. Un foglio di calcolo per la contabilità interna probabilmente non eleva la questione a questo livello. Il fascicolo penale di un cliente, la cartella clinica, la busta paga dei dipendenti, sì. La proporzionalità è legittima; l'inerzia collettiva con cui la PMI europea è rimasta legata a fornitori statunitensi per tutto —anche per le questioni più sensibili— non lo è.

Schrems II compie sei anni questo luglio. La sentenza non ha cambiato le abitudini quotidiane della maggior parte delle imprese europee. Ha cambiato, però, la mappa dei rischi a cui tali imprese sono esposte. Quando una decisione amministrativa statunitense si interpone tra il regolamento europeo e l'operatività reale di una PMI, conviene almeno sapere che tale decisione esiste ed è fragile. Chi di noi ha scelto un'architettura senza intermediari —il filo conduttore di Cuadernos Lacre— preferirebbe non dover scrivere questo tipo di analisi ogni volta che uno Schrems decide di presentare un ricorso. Ma continueremo a farlo.

Fonti e letture aggiuntive

- Corte di Giustizia dell'Unione Europea — sentenza del 16 luglio 2020, causa C-311/18, *Data Protection Commissioner contro Facebook Ireland Ltd e Maximillian Schrems*.
- Regolamento (UE) 2016/679, Capo V, articoli da 44 a 50 — trasferimenti internazionali di dati personali.
- Decisione di Esecuzione (UE) 2023/1795 della Commissione, del 10 luglio 2023, sull'adeguatezza del livello di protezione dei dati personali garantito dal quadro UE-USA per la privacy dei dati (EU-US Data Privacy Framework).
- Comitato europeo per la protezione dei dati — *Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE*, adottate il 18 giugno 2021.
- noyb.eu — denuncia presentata il 7 settembre 2023 contro la Decisione (UE) 2023/1795 presso le autorità europee di protezione dei dati.
- *Foreign Intelligence Surveillance Act*, sezione 702 (codificata in 50 U.S.C. § 1881a), e Ordine Esecutivo 12333 sulle attività di intelligence statunitense al di fuori del territorio nazionale.

← PrecedenteQuando non c'è nessuno in mezzoSuccessivo →CUADERNOS_LIST_SHA256_TITLE

Letture recenti

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Porta questo articolo dove ne hai bisogno.

↓ Markdown ↓ Testo semplice ↓ PDF

Il file viene scaricato sul tuo dispositivo. Da lì puoi salvarlo, importarlo in Solo2 o condividerlo come preferisci. Cuadernos non decide la destinazione per te.

Sigillo di cera · SHA-256 3dbf8a4ecbe3e1824a7dce0c5d71ae45121e5f8ad0842de31f0b49237b978506

Cuadernos Lacre · Una pubblicazione di Menzuri Gestión S.L. ·
scritta da R.Eugenio · a cura del team di Solo2.