Schrems II, cinci ani mai târziu

Sentința care a schimbat dreptul transferurilor internaționale de date cu caracter personal. Cinci ani mai târziu, o parte considerabilă a activității cotidiene europene continuă să funcționeze ca și cum nimic nu s-ar fi întâmplat.

Să ne înțelegem: Pe 16 iulie 2020, într-o dimineață de joi, un tribunal european a declarat ilegală o parte enormă din modul în care companiile îți trimiteau datele în Statele Unite. Cinci ani mai târziu, aproape nimeni nu a schimbat nimic. Informațiile tale continuă să zboare exact ca atunci.

Sentința care a avut nevoie de trei ore pentru a schimba regulile

Pe 16 iulie 2020, în jurul orei zece și un sfert dimineața, ora Luxemburgului, Curtea de Justiție a Uniunii Europene a făcut publică sentința în cauza C-311/18. În următoarele trei ore, regimul juridic care susținea transferul zilnic de date cu caracter personal din Europa către Statele Unite — așa-numitul Scut de Confidențialitate, Privacy Shield în denumirea sa oficială — a încetat să mai existe. Când responsabilii europeni cu protecția datelor și-au terminat prânzul în acea zi, cadrul sub care companiile și administrațiile lor operau nu mai era valabil.

Sentința este cunoscută astăzi sub numele de Schrems II, după Maximilian Schrems, activistul austriac a cărui plângere împotriva Facebook Ireland a declanșat procesul. Plângerea, în mod concret, viza transferurile dintre Facebook Irlanda și Facebook Statele Unite. Sentința, în mod general, merge mult mai departe: dictează cum și în ce condiții pot fi transferate în Statele Unite orice date cu caracter personal colectate pe teritoriul european.

Aproape șase ani mai târziu, cadrul de înlocuire există — EU-US Data Privacy Framework, adoptat în iulie 2023 — și se află, de asemenea, sub presiune juridică. O nouă rundă Schrems se pregătește. Între timp, întreprinderile mici și mijlocii europene continuă să folosească servicii cloud americane pentru sarcini cotidiene, majoritatea fără să știe că problema juridică pe care se bazează aceste servicii rămâne deschisă.

Ce spunea exact Schrems II

Sentința se bazează pe trei piese. Prima este Carta Drepturilor Fundamentale a Uniunii Europene, în special articolele 7 (viața privată și de familie), 8 (protecția datelor cu caracter personal) și 47 (dreptul la o cale de atac eficientă). A doua este Regulamentul General privind Protecția Datelor — RGPD pe care mulți europeni și-l amintesc doar prin notificările de cookie-uri —, în special capitolul V, articolele 44-50, privind transferurile internaționale. A treia este legislația americană de informații: secțiunea 702 din Foreign Intelligence Surveillance Act, FISA 702 în jargon juridic, și Ordinul Executiv prezidențial 12333.

Curtea a procedat prin contrast. Carta Drepturilor Fundamentale cere ca datele cu caracter personal ale cetățenilor europeni să beneficieze, atunci când părăsesc Uniunea, de un nivel de protecție esențialmente echivalent cu cel garantat de RGPD. Întrebarea era, prin urmare, dacă Statele Unite oferă acest nivel esențialmente echivalent.

Răspunsul a fost negativ, și nu din cauza unor nuanțe. FISA 702 permite guvernului american să colecteze comunicațiile persoanelor non-americane aflate în afara teritoriului național fără autorizație judiciară individuală

prealabilă, fără notificarea persoanei vizate și fără o cale de atac eficientă comparabilă cu cea europeană. Ordinul Executiv 12333 extinde această capacitate în mod analog în afara teritoriului național. Curtea a concluzionat că cetățeanul european, în fața sistemului juridic american, nu dispune de protecția esențialmente echivalentă pe care o cere Carta. Echivalența, prin urmare, nu există.

De aici consecința directă: Decizia 2016/1250 a Comisiei Europene, care validase Privacy Shield ca cadru adecvat pentru transferuri, a fost declarată nevalidă. Orice transfer bazat exclusiv pe acel cadru a rămas fără bază juridică din acel moment.

Ce a supraviețuit (și în ce condiții)

Schrems II nu a eliminat toate instrumentele. Clauzele Contractuale Standard — SCC în jargon internațional, după inițialele englezești Standard Contractual Clauses — au supraviețuit. Acestea sunt contracte-model aprobate de Comisia Europeană: un exportator european și un importator din țara de destinație le semnează angajându-se să prelucreze datele conform standardului european. Compania care a crezut că a rezolvat problema pe 17 iulie 2020 a semnat SCC cu furnizorul său și s-a declarat mulțumită.

Disconfortul a apărut la citirea atentă a sentinței. Curtea a clarificat că SCC rămân valabile, dar valabilitatea lor depinde de o condiție care merită subliniată: ca importatorul datelor să le poată respecta în practică. Dacă legislația națională a țării de destinație îl împiedică să respecte clauzele — deoarece, de exemplu, un ordin sub FISA 702 îl obligă să predea datele fără a-și notifica partenerul european —, clauzele nu protejează în realitate. Și atunci, spune Curtea, exportatorul european trebuie să suspende transferul.

Acest lucru a introdus un nou obiect în practica europeană de protecție a datelor: Transfer Impact Assessment, sau analiza impactului transferului, cunoscută sub acronimul englezesc TIA. De fiecare dată când o companie europeană dorește să transfere date în Statele Unite sub egida SCC, trebuie să evalueze formal dacă destinatarul poate respecta clauzele având în vedere legislația care i se aplică. Comitetul European pentru Protecția Datelor a publicat orientări detaliate despre cum se realizează TIA. Practica onestă dă de obicei același rezultat: dacă importatorul este o filială americană a unui gigant cloud, răspunsul sincer la TIA este că clauzele nu pot fi respectate așa cum sunt scrise.

Privacy Framework și viitorul Schrems III

Pe 10 iulie 2023, Comisia Europeană a adoptat o nouă Decizie de Adecvare: 2023/1795. Aceasta înlocuiește defunctul Privacy Shield și funcționează sub numele EU-US Data Privacy Framework. Statele Unite și-au modificat anterior regimul intern prin Ordinul Executiv 14086, care limitează sfera de aplicare a inteligenței semnalelor la ceea ce este „necesar și proporțional” — terminologie familiară cititorului european, nu atât de mult practicii administrative americane — și creează un organ de revizuire numit Data Protection Review Court (DPRC). Comisia a considerat că aceste modificări au fost suficiente pentru a restabili nivelul esențialmente echivalent.

Organizația noyb, fondată de Schrems, a depus o plângere pe 7 septembrie 2023 împotriva noii Decizii. Argumentele sunt cele așteptate: DPRC nu este un tribunal independent în sensul articolului 47 din Cartă; conceptele de „necesar și proporțional” nu traduc mecanic standardele europene; și, în sfârșit, o protecție care se bazează pe un Ordin Executiv poate fi revocată de următorul Ordin Executiv. O sentință a CJEU privind noua Decizie — pe care mulți o numesc deja, cu o anumită resemnare, Schrems III — este așteptată în următorii ani. Rezultatul nu poate fi anticipat. Structura argumentului, în orice caz, seamănă foarte mult cu cea din 2020.

Ce nu aude IMM-ul european

În timp ce marea cameră a CJEU deliberează, biroul de avocatură de dimensiuni medii continuă să schimbe corespondență cu clienții săi prin Microsoft 365 găzduit în regiuni europene, dar deținut de o companie

americană supusă FISA 702. Cabinetul medical privat sincronizează agendele prin Google Workspace. Consultantul fiscal trimite declarații semnate prin DocuSign. Psihologul facturează dintr-un tabel în Notion. Biroul de avocatură specializat în dreptul muncii arhivează dosare în Dropbox. Și practic toți aceștia, în plus, își deservesc clienții prin WhatsApp. Toate acestea pot funcționa sub umbrela, conform furnizorilor, Deciziei de Adecvare 2023/1795. În ziua în care această Decizie va cădea în Schrems III, toate aceste relații rămân expuse în aceeași secundă.

Problema nu este retorică. În între 2022 și 2024, mai multe autorități europene au soluționat dosare împotriva operatorilor pentru utilizarea Google Analytics fără un instrument adecvat de transfer, aplicând literal raționamentul CJEU chiar înainte ca Privacy Framework să intre în vigoare. Autoritatea franceză, CNIL, a fost prima care a formalizat criteriul în 2022; autoritățile austriacă, italiană și altele au urmat la scurt timp. Nerespectarea, sub actualul design operațional al IMM-ului european, se documentează în timp real în fața oricui știe unde să privească.

TIA ca instrument, nu ca ritual

O parte considerabilă a TIA-urilor care circulă prin birourile europene sunt, citite cu atenție, exerciții formale. Enumeră instrumentele contractuale, certificările furnizorului, citează garanțiile tehnice, bifează căsuța. Puține se întreabă serios dacă un ordin FISA 702 ar obliga furnizorul să predea datele. Și mai puține se întreabă ce s-ar întâmpla cu acel transfer sub o ipotetică revizuire a Privacy Framework. Articolul 5 din RGPD cere operatorului să fie capabil să demonstreze conformitatea. O TIA care nu este făcută serios nu demonstrează nimic; ceea ce demonstrează este voința de a se conforma pe hârtie în timp ce în practică se face contrariul.

Versiunea sinceră a TIA începe cu o întrebare simplă: ce s-ar întâmpla dacă mâine i-ar parveni acestui furnizor un ordin FISA 702 privind aceste date specifice? Dacă răspunsul onest este „ar trebui să le predea fără să ne anunțe”, clauzele contractuale nu rezolvă problema. Ceea ce o rezolvă, în cazurile în care întrebarea contează cu adevărat, este să nu fi pus datele în mâinile acelui furnizor.

Schimbarea politică ca risc structural

Există un strat suplimentar, politic, care merită numit fără dramatism. Decizia de Adecvare 2023/1795 se bazează, în ultimă instanță, pe Ordinul Executiv 14086, semnat de președintele Biden în octombrie 2022. Un Ordin Executiv este semnat de un președinte și poate fi revocat, modificat sau golit de conținut de următorul. Protecția datelor europene în Statele Unite depinde, astfel, de o decizie administrativă pe care nici Congresul american nu o garantează, nici sistemul juridic american nu o protejează cu soliditatea cu care protejează alte materii interne. Din ianuarie 2025, o nouă administrație guvernează Statele Unite, iar întrebarea privind continuitatea practică a EO 14086 a încetat să mai fie o ipoteză pentru a deveni contemporană. Orice scenariu în care administrația decide să retragă sau să atenueze Ordinul ar lăsa Decizia Europeană fără piesa pe care a fost construită.

Nu este un argument conspirativ. Este lectura sobră a designului juridic. Cadrele de protecție a datelor transatlantice au căzut deja de două ori: Safe Harbor în 2015 (sentința Schrems I), Privacy Shield în 2020 (Schrems II). Al treilea se bazează pe o piesă mai fragilă decât cei doi predecesori ai săi. O companie europeană care își pariază astăzi prelucrarea datelor pe acea piesă ia o decizie de gestionare a riscului, nu de simplă conformitate normativă.

Pentru cititorul profesionist

Întrebările operaționale care merită formulate înainte de a alege un serviciu cloud pentru date profesionale — cu rigoarea cu care un inspector de protecție a datelor le-ar pune — sunt următoarele:

1. Unde sunt stocate fizic datele? O regiune europeană nu este un răspuns suficient dacă operatorul este american.
2. Cine operează serviciul, în ce jurisdicție este încorporat și la ce ordine legale poate fi supus?
3. Ce instrument de transfer este invocat: Decizia de Adecvare 2023/1795, SCC cu TIA, derogarea de la articolul 49 din RGPD? Este defendabilă această alegere în fața unei inspecții?
4. Dacă Decizia de Adecvare ar cădea mâine, ce plan operațional există pentru a menține activitatea?
5. Există o alternativă europeană sau auto-găzduită pentru acea funcție și care ar fi costul real al migrării?

Nu toate funcțiile biroului cotidian necesită același răspuns. Un tabel pentru contabilitate internă probabil nu ridică întrebarea la acest nivel. Dosarul penal al unui client, istoricul medical, statul de plată al angajaților, da. Proporționalitatea este legitimă; inerția colectivă cu care IMM-ul european a rămas la furnizori americani pentru tot — inclusiv pentru cele mai sensibile lucruri — nu este.

Schrems II împlinește șase ani în acest iulie. Sentința nu a schimbat obiceiurile cotidiene ale majorității companiilor europene. A schimbat, în schimb, harta riscurilor la care aceste companii sunt expuse. Când o decizie administrativă americană se interpune între regulamentul european și activitatea reală a unui IMM, este bine să știm cel puțin că decizia este acolo și că este fragilă. Cei dintre noi care au ales o arhitectură fără operator la mijloc — firul care străbate Cuadernos Lacre — am prefera să nu trebuiască să scriem acest tip de analiză de fiecare dată când un Schrems se decide să depună un recurs. Dar vom continua să o facem.

Notă editorială: când aceste Cuadernos numesc companii sau produse, nu este pentru a acuza. Cei care le construiesc fac o muncă pe care milioane de oameni o folosesc și o apreciază. Ceea ce subliniem este structural — modelul, nu marca. Mărcile apar ca exemplu pentru că sunt cele pe care cititorul le recunoaște.

Surse și lecturi suplimentare

- Curtea de Justiție a Uniunii Europene — sentința din 16 iulie 2020, cauza C-311/18, *Data Protection Commissioner împotriva Facebook Ireland Ltd. și Maximillian Schrems*.
- Regulamentul (UE) 2016/679, capitolul V, articolele 44-50 — transferurile internaționale de date cu caracter personal.
- Decizia de punere în aplicare (UE) 2023/1795 a Comisiei din 10 iulie 2023 privind nivelul adecvat de protecție a datelor cu caracter personal în cadrul EU-US Data Privacy Framework.
- Comitetul European pentru Protecția Datelor — *Recomandările 01/2020 privind măsurile care completează instrumentele de transfer pentru a asigura respectarea nivelului de protecție a datelor cu caracter personal al UE*, adoptate la 18 iunie 2021.
- noyb.eu — plângere depusă la 7 septembrie 2023 împotriva Deciziei (UE) 2023/1795 în fața autorităților europene de protecție a datelor.
- *Foreign Intelligence Surveillance Act*, secțiunea 702 (codificată în 50 U.S.C. § 1881a), și Ordinul Executiv 12333 privind activitățile de informații americane în afara teritoriului național.

← PrecedentCând nu este nimeni la mijlocUrmător →Ce este cu adevărat SHA-256

Lecturi recente

- Analiză · 18 mai 2026 Confidențialitate reală vs. aparentă: întrebările pe care e bine să ți le pui
- Analiză · 18 mai 2026 Self-hosting ca practică profesională
- Concept · 18 mai 2026 Cele 24 de cuvinte: ce este o identitate criptografică

Luați acest articol cu dumneavoastră oriunde aveți nevoie.

↓ Markdown ↓ Text simplu ↓ PDF

Fişierul se va descărca pe dispozitivul dumneavoastră. De acolo îl puteţi salva, importa în Solo2 sau partaja oriunde doriți. Cuadernos nu decide destinația în locul dumneavoastră.

Sigiliu de ceară · SHA-256 3f9cbac5b87ee472510143d1872563f8eae89c3584b15d998390e69d564d7219

Cuadernos Lacre · O publicație a Menzuri Gestión S.L. ·
scrisă de R.Eugenio · editată de echipa Solo2.