Schrems II, cinq ans après

L'arrêt qui a changé le droit des transferts internationaux de données à caractère personnel. Cinq ans plus tard, une part considérable du quotidien des bureaux européens continue de fonctionner comme si de rien n'était.

Pour faire simple : Le 16 juillet 2020, un jeudi matin, un tribunal européen a déclaré illégale une part énorme de la manière dont les entreprises envoyaient vos données aux États-Unis. Cinq ans plus part, presque rien n'a changé. Vos informations continuent de voyager exactement comme à l'époque.

L'arrêt qui a mis trois heures à changer les règles

Le 16 juillet 2020, vers dix heures et quart du matin, heure de Luxembourg, la Cour de justice de l'Union européenne (TJUE) a rendu public l'arrêt dans l'affaire C-311/18. Dans les trois heures qui ont suivi, le régime juridique qui soutenait le transfert quotidien de données à caractère personnel de l'Europe vers les États-Unis — le fameux Privacy Shield (Bouclier de protection des données) — a cessé d'exister. Lorsque les responsables de la protection des données européens ont fini de déjeuner ce jour-là, le cadre dans lequel leurs entreprises et administrations opéraient n'était plus valide.

L'arrêt est connu aujourd'hui sous le nom de Schrems II, d'après Maximilian Schrems, l'activiste autrichien dont la plainte contre Facebook Ireland l'a déclenché. La plainte, concrètement, portait sur les transferts entre Facebook Irlande et Facebook États-Unis. L'arrêt, de manière générale, va beaucoup plus loin : il dicte comment et sous quelles conditions toute donnée à caractère personnel collectée sur le territoire européen peut être transférée aux États-Unis.

Près de six ans plus tard, le cadre de remplacement existe — l'EU-US Data Privacy Framework, adopté en juillet 2023 — et se trouve lui aussi sous pression juridique. Une nouvelle ronde Schrems se prépare. Pendant ce temps, la petite et moyenne entreprise européenne continue d'utiliser des services cloud américains pour ses tâches quotidiennes, ignorant pour la plupart que la question juridique sur laquelle reposent ces services reste ouverte.

Ce que disait exactement Schrems II

L'arrêt repose sur trois piliers. Le premier est la Charte des droits fondamentaux de l'Union européenne, en particulier ses articles 7 (vie privée et familiale), 8 (protection des données à caractère personnel) et 47 (droit à un recours effectif). Le second est le Règlement général sur la protection des données — le RGPD que beaucoup d'Européens ne connaissent qu'à travers les bannières de cookies —, spécifiquement son chapitre V, articles 44 à 50, sur les transferts internationaux. Le troisième est la législation américaine en matière de renseignement : la section 702 du Foreign Intelligence Surveillance Act, FISA 702 dans le jargon juridique, et l'Executive Order présidentiel 12333.

La Cour a procédé par comparaison. La Charte des droits fondamentaux exige que les données à caractère personnel des citoyens européens bénéficient, lorsqu'elles quittent l'Union, d'un niveau de protection substantiellement équivalent à celui garanti par le RGPD. La question était par conséquent de savoir si les États-Unis offraient ce niveau substantiellement équivalent.

La réponse a été négative, et pas seulement sur des nuances. Le FISA 702 permet au gouvernement américain de collecter les communications de non-Américains situés hors du territoire national sans autorisation judiciaire individuelle préalable, sans notification à la personne concernée et sans recours effectif comparable au système européen. L'Executive Order 12333 étend cette capacité de manière analogue hors du territoire national. La Cour a conclu que le citoyen européen, face au système juridique américain, ne dispose pas de la protection substantiellement équivalente exigée par la Charte. L'équivalence n'existe donc pas.

D'où la conséquence directe : la décision 2016/1250 de la Commission européenne, qui avait validé le Privacy Shield comme cadre adéquat pour les transferts, a été déclarée invalide. Tout transfert fondé uniquement sur ce cadre s'est retrouvé sans base juridique à l'instant même.

Ce qui a survécu (et sous quelles conditions)

Schrems II n'a pas supprimé tous les instruments. Les Clauses Contractuelles Types — les SCC dans le jargon international — ont survécu. Ce sont des contrats modèles approuvés par la Commission européenne : un exportateur européen et un importateur du pays de destination les signent en s'engageant à traiter les données selon le standard européen. L'entreprise qui pensait avoir résolu le problème le 17 juillet 2020 a signé des SCC avec son fournisseur et s'est estimée satisfaite.

L'inconfort est apparu en lisant l'arrêt attentivement. La Cour a précisé que les SCC restent valides, mais leur validité dépend d'une condition qu'il convient de souligner : que l'importateur des données puisse les respecter dans la pratique. Si la législation nationale du pays de destination l'empêche de respecter les clauses — parce que, par exemple, une injonction sous FISA 702 l'oblige à livrer les données sans en informer sa contrepartie européenne —, les clauses ne protègent en réalité rien. Et alors, dit la Cour, l'exportateur européen doit suspendre le transfert.

Cela a introduit un nouvel objet dans la pratique européenne de la protection des données : la Transfer Impact Assessment, ou analyse d'impact du transfert, connue sous son acronyme anglais TIA. Chaque fois qu'une entreprise européenne souhaite transférer des données aux États-Unis sous le couvert des SCC, elle doit évaluer formellement si le destinataire peut respecter les clauses compte tenu de la législation qui lui est applicable. Le Comité européen de la protection des données (EDPB) a publié des orientations détaillées sur la manière de mener la TIA. La pratique honnête donne généralement le même résultat : si l'importateur est une filiale américaine d'un géant du cloud, la réponse sincère à la TIA est que les clauses ne peuvent pas être respectées telles qu'elles sont écrites.

Le Privacy Framework et le Schrems III en attente

Le 10 juillet 2023, la Commission européenne a adopté une nouvelle Décision d'Adéquation : la 2023/1795. Elle remplace le défunt Privacy Shield et opère sous le nom d'EU-US Data Privacy Framework. Les États-Unis avaient préalablement modifié leur régime interne par l'Executive Order 14086, qui limite la portée du renseignement d'origine électromagnétique à ce qui est « nécessaire et proportionné » — une terminologie familière pour le lecteur européen, moins pour la pratique administrative américaine — et crée un organe de révision appelé Data Protection Review Court (DPRC). La Commission a considéré que ces modifications suffisaient à rétablir le niveau de protection substantiellement équivalent.

L'organisation noyb, fondée par Schrems, a déposé une plainte le 7 septembre 2023 contre la nouvelle décision. Les arguments sont ceux attendus : le DPRC n'est pas un tribunal indépendant au sens de l'article 47 de la Charte ; les concepts de « nécessaire et proportionné » ne traduisent pas mécaniquement les standards européens ; et enfin, une protection qui repose sur un Executive Order peut être révoquée par l'Executive Order suivant. Un arrêt de la TJUE sur la nouvelle décision — que beaucoup appellent déjà, avec une certaine résignation, Schrems III — est attendu pour les prochaines années. Le résultat ne peut être anticipé. La structure de l'argument, en tout cas, rappelle beaucoup celle de 2020.

Ce que la PME européenne n'entend pas

Pendant que la grande chambre de la TJUE délibère, le cabinet d'avocats de taille moyenne continue d'échanger des courriers avec ses clients via Microsoft 365 hébergé dans des régions européennes mais appartenant à une entreprise américaine soumise au FISA 702. Le cabinet médical privé synchronise ses agendas via Google Workspace. Le conseiller fiscal envoie des déclarations signées via DocuSign. Le psychologue facture à partir d'un tableur sur Notion. Le cabinet d'avocats en droit du travail archive ses dossiers sur Dropbox. Et pratiquement tous communiquent avec leurs clients par WhatsApp. Tout cela peut fonctionner sous le couvert, selon les fournisseurs, de la Décision d'Adéquation 2023/1795. Le jour où cette décision tombera dans Schrems III, toutes ces relations se retrouveront à découvert en une seconde.

La question n'est pas rhétorique. Entre 2022 et 2024, plusieurs autorités européennes ont sanctionné des responsables de traitement pour l'utilisation de Google Analytics sans instrument de transfert adéquat, en application littérale du raisonnement de la TJUE avant même l'entrée en vigueur du Privacy Framework. L'autorité française, la CNIL, a été la première à formaliser ce critère en 2022 ; les autorités autrichienne, italienne et d'autres ont suivi peu après. Le non-respect, dans la conception opérationnelle actuelle de la PME européenne, est documenté en temps réel pour qui sait regarder.

La TIA comme instrument, pas comme rituel

Une part considérable des TIA qui circulent dans les cabinets européens sont, lues avec attention, des exercices de forme. Elles listent les instruments contractuels, énumèrent les certifications du fournisseur, citent les garanties techniques, cochent la case. Rares sont celles qui se demandent sérieusement si une injonction FISA 702 obligerait le fournisseur à livrer les données. Moins encore se demandent ce qu'il adviendrait de ce transfert sous une hypothétique révision du Privacy Framework. L'article 5 du RGPD exige du responsable du traitement qu'il soit capable de démontrer la conformité. Une TIA qui n'est pas faite sérieusement ne démontre rien ; elle démontre la volonté de se conformer sur le papier tout en faisant le contraire dans la pratique.

La version sincère de la TIA commence par une question simple : que se passerait-il si ce fournisseur recevait demain une injonction FISA 702 concernant ces données précises ? Si la réponse honnête est « il devrait les livrer sans nous en informer », les clauses contractuelles ne résolvent pas le problème. Ce qui le résout, dans les cas où la question compte vraiment, c'est de ne pas avoir confié la donnée à ce fournisseur.

Le changement politique comme risque structurel

Il existe une couche supplémentaire, politique, qu'il convient de nommer sans dramatisation. La Décision d'Adéquation 2023/1795 repose, en dernier lieu, sur l'Executive Order 14086, signé par le président Biden en octobre 2022. Un Executive Order est signé par un président et peut être révoqué, modifié ou vidé de sa substance par le suivant. La protection des données européennes aux États-Unis dépend ainsi d'une décision administrative que ni le Congrès américain ne garantit, ni le système juridique américain ne protège avec la solidité avec laquelle il protège d'autres matières internes. Depuis janvier 2025, une nouvelle administration dirige les États-Unis, et la question de la continuité pratique de l'EO 14086 a cessé d'être une hypothèse pour devenir contemporaine. Tout scénario dans lequel l'administration déciderait de retirer ou d'atténuer l'Ordre laisserait la décision européenne sans la pièce sur laquelle elle a été construite.

Ce n'est pas un argument conspirationniste. C'est la lecture sobre de la conception juridique. Les cadres de protection des données transatlantiques sont déjà tombés deux fois : le Safe Harbor en 2015 (arrêt Schrems I), le Privacy Shield en 2020 (Schrems II). Le troisième repose sur une pièce plus fragile que ses deux prédécesseurs. Une entreprise européenne qui parie aujourd'hui son traitement de données sur cette pièce prend une décision de gestion des risques, et non de simple conformité réglementaire.

Pour le lecteur professionnel

Les questions opérationnelles qu'il convient de se poser avant de choisir un service cloud pour des données professionnelles — avec la rigueur qu'un inspecteur de la protection des données y mettrait — sont les suivantes :

1. Où les données sont-elles stockées physiquement ? Une région européenne n'est pas une réponse suffisante si l'opérateur est américain.
2. Qui exploite le service, dans quelle juridiction est-il constitué et à quels ordres légaux peut-il être soumis ?
3. Quel instrument de transfert est invoqué : Décision d'Adéquation 2023/1795, SCC avec TIA, dérogation de l'article 49 du RGPD ? Ce choix est-il défendable lors d'une inspection ?
4. Si la Décision d'Adéquation tombait demain, quel plan opérationnel existe-t-il pour maintenir l'activité ?
5. Existe-t-il une alternative européenne ou auto-hébergée pour cette fonction, et quel serait le coût réel d'une migration ?

Toutes les fonctions du quotidien du cabinet ne requièrent pas la même réponse. Un tableur pour la comptabilité interne n'élève probablement pas la question à ce niveau. Le dossier pénal d'un client, le dossier médical, la fiche de paie des employés, oui. La proportionnalité est légitime ; l'inertie collective avec laquelle la PME européenne est restée chez des fournisseurs américains pour tout — même pour le plus sensible — ne l'est pas.

Schrems II fête ses six ans en juillet. L'arrêt n'a pas changé les habitudes quotidiennes de la plupart des entreprises européennes. Il a cependant modifié la cartographie des risques auxquels ces entreprises sont exposées. Lorsqu'une décision administrative américaine s'interpose entre le règlement européen et le fonctionnement réel d'une PME, il convient au moins de savoir que la décision existe et qu'elle est fragile. Nous qui avons choisi une architecture sans intermédiaire — le fil conducteur de Cuadernos Lacre — préférerions ne pas avoir à rédiger ce genre d'analyse chaque fois qu'un Schrems dépose un recours. Mais nous continuerons à le faire.

Note éditoriale : quand ces Cuadernos nomment des entreprises ou des produits, ce n'est pas pour accuser. Ceux qui les construisent font un travail que des millions de personnes utilisent et apprécient. Ce que nous soulignons est structurel — le modèle, pas la marque. Les marques apparaissent comme exemples car ce sont celles que le lecteur reconnaît.

Sources et lectures complémentaires

- Cour de justice de l'Union européenne — arrêt du 16 juillet 2020, affaire C-311/18, *Data Protection Commissioner contre Facebook Ireland Ltd et Maximillian Schrems*.
- Règlement (UE) 2016/679, chapitre V, articles 44 à 50 — transferts internationaux de données à caractère personnel.
- Décision d'exécution (UE) 2023/1795 de la Commission, du 10 juillet 2023, constatant le niveau de protection adéquat des données à caractère personnel assuré par l'EU-US Data Privacy Framework.
- Comité européen de la protection des données — *Recommandations 01/2020 sur les mesures qui complètent les instruments de transfert pour garantir le respect du niveau de protection des données à caractère personnel de l'UE*, adoptées le 18 juin 2021.
- noyb.eu — plainte déposée le 7 septembre 2023 contre la décision (UE) 2023/1795 auprès des autorités européennes de protection des données.
- *Foreign Intelligence Surveillance Act*, section 702 (codifiée en 50 U.S.C. § 1881a), et Executive Order 12333 sur les activités de renseignement américaines hors du territoire national.

← PrécédentQuand il n'y a personne au milieuSuivant →Ce qu'est réellement SHA-256

Lectures recentes

- Analyse · 18 mai 2026 Confidentialité réelle vs apparente : les questions à se poser
- Analyse · 18 mai 2026 Self-hosting comme pratique professionnelle

- Concept · 18 mai 2026 Les 24 mots : qu'est-ce qu'une identité cryptographique

Emportez cet article où vous en avez besoin.

↓ Markdown ↓ Texte brut ↓ PDF

Le fichier est téléchargé sur votre appareil. À partir de là, vous pouvez l'enregistrer, l'importer dans Solo2 ou le partager comme vous le souhaitez. Cuadernos ne décide pas de la destination pour vous.

Cachet de cire · SHA-256 4ef6bbe8109a78255a774dcd90bab5d0f6f98b48681fa7ebdca7efcd0174c1d6

Cuadernos Lacre · Une publication de Menzuri Gestión S.L. ·
écrite par R.Eugenio · éditée par l'équipe de Solo2.