_swissprivacy.law

Trump v. Slaughter, quel avenir pour le EU-US Data Privacy Framework ?

Anna Ploix, le 15 juillet 2026

Le 29 juin 2026, la Cour suprême des États-Unis a jugé, dans l'arrêt *Trump v. Slaughter*, que la protection dont bénéficiait les commissaires de la *Federal Trade Commission* (FTC) contre une révocation discrétionnaire du Président était contraire à la Constitution américaine. Dans la mesure où l'indépendance de la FTC constitue l'un des piliers sur lesquels repose la décision d'adéquation de la Commission européenne relative à l'*EU-US Data Privacy Framework* (DPF), cette décision américaine relance, les interrogations sur la pérennité des instruments de transfert transatlantique de données personnelles.

Jugement de l'*US Supreme Court, Donald J. Trump, President of the United States, et Al, Petitioners v. Rebecca Kelly Slaughter (609 U. S.)*, du 29 juin 2026

I. Contexte

A. Que s'est-il passé pour que la Cour suprême en arrive à ce jugement ?

Peu après le début de son second mandat, en janvier 2025, le président Donald Trump a révoqué les deux commissaires démocrates alors en fonction à la FTC, Rebecca Slaughter et Alvaro Bedoya, sans invoquer l'un des motifs prévus par la loi instituant la FTC, le Federal Trade Commission Act de 1914 (« inefficacité, négligence dans l'exercice de ses fonctions ou faute grave »). Il leur a indiqué que leur maintien en fonction était incompatible avec les priorités de son administration et a fondé leur révocation directement sur l'article II de la Constitution.

Rebecca Slaughter a saisi les tribunaux fédéraux, faisant valoir que sa révocation était *ultra vires*, contraire à l'*Administrative Procedure Act* et inconstitutionnelle. Le tribunal de district lui a donné raison en s'appuyant sur le précédent *Humphrey's Executor v. United States* (1935), qui avait précisément soustrait les commissaires de la FTC à la règle de la révocation discrétionnaire posée quelques années plus tôt dans *Myers v. United States* (1926). La Cour suprême s'est ensuite saisie de l'affaire avant même l'arrêt d'appel (*certiorari before judgment*) et a rendu sa décision le 29 juin 2026. Le recours à cette procédure exceptionnelle (réservée aux affaires jugées d'une importance publique impérieuse) signale la volonté de la

Cour de trancher rapidement et directement le sort du précédent *Humphrey's Executor*, plutôt que de laisser la question mûrir devant les juridictions inférieures.

B. En quoi la FTC est-elle essentielle pour le Data Privacy Framework ?

Depuis 1995, le droit de l'Union Européenne interdit par principe l'exportation de données personnelles vers des pays tiers, sauf à ce qu'un niveau de protection adéquat y soit garanti. Faute de loi fédérale américaine générale sur la protection des données, la Commission européenne a, depuis 2000, construit à trois reprises un mécanisme d'auto-certification volontaire pour les entreprises américaines : le *Safe Harbor* (2000), le *Privacy Shield* (2016), puis l'actuel *EU-US Data Privacy Framework* (2023). Dans chacune de ses versions, ce mécanisme repose sur l'engagement des entreprises adhérentes à respecter des principes de protection des données, sous la surveillance et le pouvoir de sanction de la FTC.

Or l'art. 16(2) TFUE et l'art. 8(3) de la Charte des droits fondamentaux de l'UE exigent que le contrôle du respect des règles de protection des données soit assuré par une autorité indépendante. C'est cette exigence que la Commission a cherché à satisfaire, côté américain, en s'appuyant sur le statut alors protégé des commissaires de la FTC.

II. Résumé de la décision de la Cour

Sous la plume de John G. Roberts, la majorité de la Cour Suprême part de l'article II de la Constitution qui confie « le pouvoir exécutif » à une seule personne, le Président, à charge pour lui de veiller à la fidèle exécution des lois. De ce choix des Constituants en faveur d'un exécutif unitaire découle, selon la Cour, la nécessité que tous les fonctionnaires exerçant une partie du pouvoir exécutif restent révocables à la discrétion du Président (seule condition, à leurs yeux, permettant de maintenir la chaîne de responsabilité démocratique jusqu'au peuple). La Cour retrace cette lecture depuis la « décision de 1789 » du premier Congrès jusqu'à l'arrêt *Myers* de 1926, qui avait consacré le pouvoir de révocation discrétionnaire du Président sur les fonctionnaires exécutifs.

Restait l'obstacle du précédent *Humphrey's Executor*, qui avait justement soustrait la FTC à cette règle en la qualifiant d'organe « quasi-législatif et quasi-judiciaire » n'exerçant « aucune part du pouvoir exécutif ». La Cour retrace comment ce précédent a été progressivement vidé de sa substance par la jurisprudence ultérieure, avant de conclure que la FTC d'aujourd'hui exerce sans conteste une part substantielle du pouvoir exécutif. Elle en tire la conclusion que le régime de révocation pour juste motif applicable aux commissaires de la FTC est contraire à la séparation des pouvoirs, et que le précédent *Humphrey's Executor* doit

être écarté.

Sur le plan strictement américain, l'arrêt ne dit donc rien de la protection des données ni des transferts internationaux. Mais sa portée pratique pour l'Union Européenne est directe : les commissaires de la FTC sont désormais révocables *ad nutum* par le Président, ce qui prive la Commission européenne de l'un des deux piliers (avec la *Data Protection Review Court (DPRC)*) sur lesquels reposait sa constatation d'adéquation du droit américain.

III. Quel futur pour le Data Privacy Framework ?

Le parallèle avec les deux précédentes révocations du cadre transatlantique est frappant. Dans l'arrêt *Schrems I* (C-362/14, 6 octobre 2015), la CJUE avait invalidé le *Safe Harbor* notamment car le droit américain ne prévoyait aucune limitation suffisante de l'accès des autorités publiques aux données, ni de voie de recours effective pour les personnes concernées. L'autorité chargée de la surveillance du système (la FTC) n'offrant pas de garanties suffisantes d'indépendance et de contrôle vis-à-vis des services de renseignement.

Dans l'arrêt *Schrems II* (C-311/18, 16 juillet 2020, cf. swissprivacy.law/17/), la CJUE avait invalidé le *Privacy Shield* en jugeant cette fois que le mécanisme de médiation censé offrir un recours aux personnes concernées ne présentait pas l'indépendance structurelle requise à l'égard du pouvoir exécutif américain. Dans les deux cas, c'est donc bien l'indépendance du mécanisme de surveillance et de recours face à l'exécutif américain qui a emporté la conviction de la CJUE.

Le *Data Privacy Framework* de 2023 avait précisément été construit pour répondre à cette double exigence : la DPRC pour le recours en matière de surveillance, la FTC pour l'exécution des engagements de conformité pris par les entreprises certifiées. Avec *Trump v. Slaughter*, c'est ce second pilier qui vient d'être fragilisé.

Ce constat ne concerne d'ailleurs pas que l'Union européenne. La Suisse dispose de son propre pendant du dispositif, le *Swiss-US Data Privacy Framework*, dont l'équivalence est reconnue par le Conseil fédéral depuis le 14 août 2024 (cf. swissprivacy.law/313/ et swissprivacy.law/332/). Ce mécanisme suisse repose sur la même architecture institutionnelle américaine que son homologue européen (la FTC comme autorité d'exécution des engagements de certification) et se trouve donc exposé, dans les mêmes termes, à la fragilisation résultant de *Trump v. Slaughter*.

Il convient toutefois de ne pas surestimer la portée immédiate de l'arrêt. La décision d'exécu-

tion de la Commission européenne reste formellement en vigueur tant qu'elle n'a pas été abrogée par la Commission elle-même ou annulée par la CJUE. Selon les informations disponibles à ce jour, la Commission a indiqué qu'elle allait examiner les implications de l'arrêt américain sur sa décision d'adéquation, sans toutefois suspendre celle-ci. De son côté, noyb (NB : organisation fondée par Maximilian Schrems) a adressé une lettre formelle à la Commission lui demandant d'engager un « retrait ordonné » du dispositif et a annoncé son intention de porter l'affaire devant la CJUE, un contentieux qui, à l'image des précédents, prendrait vraisemblablement plusieurs années avant d'aboutir à une décision définitive.

IV. Alternatives au Data Privacy Framework en Europe et en Suisse

En parallèle, un développement récent (sans lien direct avec l'arrêt *Trump v. Slaughter*) mérite attention. Le 15 avril 2026, le Comité européen de la protection des données a adopté l'Opinion 15/2026 approuvant la certification Europrivacy (le seul label européen de protection des données reconnu à ce jour au titre de l'art. 42 RGPD) comme mécanisme de garanties appropriées au sens de l'art. 46 RGPD. Cette certification, désormais également ouverte aux entités établies hors de l'Union européenne, pourrait ainsi permettre à des entreprises américaines de démontrer, indépendamment de tout constat d'adéquation étatique, qu'elles offrent des garanties appropriées pour recevoir des données en provenance de l'UE.

Pour les entités soumises au droit suisse, cette évolution ne se transpose toutefois pas automatiquement. Le transfert de données personnelles à l'étranger est régi par les art. 16 et 17 LPD et par les art. 8 à 12 de l'OPDo. En l'absence de décision du Conseil fédéral reconnaissant un niveau de protection adéquat dans l'État destinataire, l'art. 12 al. 1 OPDo permet qu'un niveau de protection approprié soit assuré par un code de conduite ou par une certification. Mais Europrivacy, en tant que label reconnu par le CEPD dans le cadre du RGPD, n'a à ce jour pas fait l'objet d'une reconnaissance équivalente en droit suisse au titre de l'art. 12 OPDo. Une entreprise américaine certifiée Europrivacy pour ses transferts au sens du RGPD ne pourrait donc pas s'en prévaloir pour justifier, sous l'angle de la LPD, la licéité d'un transfert de données depuis la Suisse.

La difficulté est plus aiguë encore pour certaines législations cantonales applicables aux institutions publiques qui interdisent purement et simplement aux institutions publiques de transférer des données personnelles à un sous-traitant établi dans un État dont le niveau de protection n'est pas jugé adéquat, sans ouvrir la possibilité de recourir à des garanties alternatives. Pour ces institutions, seule une reconnaissance d'adéquation reste susceptible d'autoriser un tel transfert.

V. Conclusion

Trump v. Slaughter ne remet pas, à lui seul, en cause l'existence juridique du *Data Privacy Framework*, la décision d'adéquation de 2023 demeure en vigueur. Deux voies pourraient toutefois mettre fin à ce régime. D'une part, la Commission dispose du pouvoir de suspendre, modifier ou abroger elle-même sa décision d'adéquation par voie d'acte d'exécution, sans devoir attendre l'intervention d'une juridiction. D'autre part, à défaut d'une telle initiative de la Commission, il faudra sans doute attendre l'issue d'un contentieux devant la CJUE pour connaître le sort définitif du dispositif.

Proposition de citation : Anna Ploix, Trump v. Slaughter, quel avenir pour le EU-US Data Privacy Framework ?, 15 juillet 2026 *in* www.swissprivacy.law/414

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.