_swissprivacy.law

Les transferts transatlantiques de données personnelles : *quo vadis* ?

Jeremy Reichlin et Livio di Tria, le 21 décembre 2022

Le Président des États-Unis d'Amérique Joe Biden a signé le 7 octobre 2022 un décret présidentiel visant à répondre aux préoccupations soulevées par la Cour de justice de l'Union européenne en matière de transferts transatlantiques de données personnelles. Ce décret présidentiel pose les jalons nécessaires à l'établissement par la Commission européenne d'une décision d'adéquation en faveur des États-Unis d'Amérique. Un projet en ce sens vient d'ailleurs d'être publié par la Commission européenne.

Point de départ

La question des transferts de données personnelles depuis l'Espace économique européen et la Suisse vers des pays tiers est un véritable casse-tête, et ce tant pour les autorités que pour les personnes privées. Cela est particulièrement tangible pour les transferts de données personnelles vers des pays tiers qui ne sont pas au bénéfice d'une décision d'adéquation.

Pour ces derniers pays, les transferts doivent être encadrés en utilisant différents outils juridiques, comme les clauses contractuelles types (qui sont en pratique l'outil le plus utilisé), les règles d'entreprise contraignantes, les codes de conduite ou les certifications. Ces outils juridiques doivent permettre d'assurer un niveau de protection des données suffisant et approprié. À ceci s'ajoutent les prescriptions supplémentaires qui doivent être prises lors du recours aux clauses contractuelles types (cf. http://www.swissprivacy.law/191 et www.swissprivacy.law/40).

Le cas spécifique des USA

Le cas des transferts de données personnelles depuis l'Espace économique européen et la Suisse vers les États-Unis d'Amérique (USA) est particulièrement épineux. Il a fait l'objet de plusieurs sursauts durant ces dernières années, en particulier avec l'invalidation par la Cour de justice de l'Union européenne (CJUE) en 2015 du « *Safe Harbor* » dans le cadre de l'affaire C-362/14 du 6 octobre 2015 (arrêt Schrems I), puis en 2020 du « Privacy Shield EU-US » dans le cadre de l'affaire C-311/18 du 16 juillet 2020 (arrêt Schrems II).

Ces deux programmes, mis en place conjointement par les représentants de l'Union européenne et des USA, reposaient sur un ensemble de principes qui permettaient à certaines entreprises étatsuniennes de certifier qu'elles respectaient la législation européenne en matière de protection des données, ce qui facilitait les transferts transatlantiques de données personnelles. Des versions suisses de ces programmes ont également été mises en place et approuvées par le PFPDT. Toutefois après l'invalidation des programmes UE-USA, les programmes suisses ont également été invalidés.

Depuis l'invalidation du « Privacy Shield EU-US », une certaine insécurité juridique règne en ce qui concerne les transferts transatlantiques de données personnelles. Cette insécurité est d'autant plus importante que la mise en œuvre des outils juridiques permettant d'assurer un niveau de protection suffisant et approprié (en particulier les clauses contractuelles types) demeure floue et controversée. Cette situation présente une contradiction avec la situation factuelle. Il est en effet estimé que les flux de données personnelles transatlantiques sont les plus élevés du monde et représentent une grande partie de la relation économique entre l'Union européenne et les USA.

Vers un nouveau cadre transatlantique ?

Conscients des enjeux, les représentants de la Maison-Blanche et de la Commission européenne annonçaient le 25 mars 2022, dans le cadre d'une conférence de presse conjointe, leur volonté commune de restaurer la situation et avoir conclu un accord de principe répondant aux préoccupations soulevées par la CJUE. Cet accord de principe restait néanmoins à être transposé du côté des USA sous la forme d'un nouveau décret présidentiel, pour permettre à la Commission européenne de fonder son analyse en vue d'un projet de décision d'adéquation.

Le 7 octobre 2022, le président Joe Biden a précisément signé l'*Executive Order on Enhancing Safeguards For United States Signals Intelligence Activities*) visant à répondre aux préoccupations de la CJUE en matière de surveillance électronique par les autorités américaines, pomme de discorde dans les arrêts Schrems I et II. Ce décret présidentiel a ainsi pour but d'offrir aux résidents de l'Espace économique européen des protections plus solides contre les activités de « *Bulk Surveillance* » (ou surveillance de masse). Il annule et remplace le précédent décret présidentiel signé en 2014 par le Président Barack Obama.

Les grandes lignes du décret présidentiel

Préalablement à l'analyse des grandes lignes du décret présidentiel, il nous semble important

de rappeler brièvement les leçons de l'arrêt Schrems II. Dans le cadre de celui-ci, la CJUE estime nécessaire – pour qu'un cadre transatlantique puisse être correctement mis en place – que les USA s'assurent notamment que :

1. la surveillance de masse par les autorités américaines soit proportionnée au sens de l'art. 52 de la Charte des droits fondamentaux de l'UE, et ;
2. toute personne dispose de voies de droit effectives pour faire valoir ses droits en matière de protection de la sphère privée et d'autodétermination informationnelle et que ces atteintes puissent être soumises à un système de contrôle efficace, indépendant et impartial, conformément à l' art. 47 de la Charte des droits fondamentaux de l'UE.

C'est dans cet esprit que le décret présidentiel a été rédigé. Nous limiterons donc notre analyse à ces deux points, bien que celui-ci intègre également d'autres changements (cf. pour une autre analyse : David Rosenthal, « EU-US Data Privacy Framework : When and how it will apply to Switzerland »).

Premièrement, la section 2 du décret présidentiel emprunte désormais la terminologie de la CJUE pour le test de proportionnalité vis-à-vis des mesures de surveillance électronique. Jusque-là, le précédent décret présidentiel prévoyait que « Signals intelligence activities shall be **as tailored as feasible** […] ». Désormais, il est prévu que les mesures de surveillance se doivent d'être « nécessaires » et « proportionnelles ». Malgré une terminologie différente, il est fort à parier que les pratiques étatsuniennes relatives à la surveillance de masse (p. ex. via leurs programmes « PRISM » ou « Upstream ») n'évoluent que marginalement, ce qui pourrait potentiellement être à nouveau critiqué par la CJUE.

Deuxièmement, la section 3 du décret présidentiel prévoit la création d'un système de contrôle afin de permettre à tout résident européen de faire valoir ses droits en matière de protection des données. La procédure devrait se faire en deux étapes successives.

La première étape est confiée au *Civil Liberties Protection Officer* (CLPO), rattaché au Bureau du Directeur du renseignement national, soit à une branche du gouvernement. Le CLPO est en charge d'enquêter sur une éventuelle plainte et de déterminer les mesures correctives appropriées, ainsi que d'informer le plaignant, sans confirmer ou infirmer que le plaignant a fait l'objet d'activités de surveillance de masse, qu'aucune violation n'a été découverte (à l'instar par exemple d'un droit d'accès indirect, comme celui prévu par l'art. 63 de la Loi fédérale sur le renseignement).

La seconde étape est quant à elle confiée au *Data Protection Review Court*. Cette dernière a pour but de fournir un rapport classifié sur les informations mettant en lumière une violation de toute autorité soumise à la surveillance du *Foreign Intelligence Surveillance Court* à l'*Attorney General Assistant* pour la sécurité nationale.

Les juges de la *Data Protection Review Court* seront nommés conjointement par l'*Attorney General* et le *Privacy and Civil Liberties Oversight Board* (PCLOB). Ils devront être des praticiens du droit ayant une expérience appropriée dans les domaines de la protection des données et de la sécurité nationale. Ils ne devront en aucun cas, durant leur nomination, être des employés du gouvernement des USA.

Il reste à déterminer, à l'aune du droit de l'UE, si ce système permet réellement de garantir les droits des personnes concernées. Ces deux entités étant vraisemblablement rattachées à la branche exécutive du gouvernement, cela pourrait potentiellement susciter le questionnement par rapport à l'indépendance requise.

Prochaines étapes

La signature du décret présidentiel va désormais permettre à la Commission européenne de rédiger un projet de décision d'adéquation en vertu de l'art. 45 RGPD. Dans ce contexte, la Commission européenne a débuté le 13 décembre 2022 le processus d'adoption d'une décision d'adéquation concernant le cadre de protection des données UE-USA en mettant en consultation un projet de décision. En substance, ce projet de décision d'adéquation considère que le décret présidentiel « provides comparable safeguards to those of the EU » sans toutefois véritablement indiqué comment la Commission européenne arrive à ce constat, notamment au regard du principe de proportionnalité.

Quoi qu'il en soit, la Commission européenne a désormais transmis son projet de décision d'adéquation au Comité européen de la protection des données (CEPD) qui a la compétence de rendre un avis concernant l'évaluation du caractère adéquat du niveau de protection assuré par un pays tiers (art. 70 par. 1 let. s RGPD). La Commission européenne devra également prendre en compte l'avis des États membres de l'UE. Néanmoins, ni l'avis du CEPD ni l'avis des États membres n'est contraignant. La fin du processus d'adoption d'une décision d'adéquation devra se terminer dans le courant de l'été 2023.

Il y a fort à parier que la décision – même si elle devait récolter les faveurs des parties concernées – soit rapidement contestée devant les tribunaux nationaux et européens. Alors même que les personnes soumises au RGPD pourront se fier à la décision, un flou juridique perdu-

rera jusqu'à la décision de la CJUE dans le cas d'une contestation. L'association « *None Of Your Business (NOYB)* » a déjà annoncé que le décret présidentiel lui semblait peu susceptible de satisfaire aux garanties européennes.

Dans le cadre du processus d'adoption (en particulier lors du processus de consultation), il est vraisemblable que la question de la densité normative du décret présentiel – soit une instruction de comportement à l'attention des administrations et non une loi au sens formel ou matériel –, respectivement l'application du principe de proportionnalité soit questionnée. Cela est d'autant plus vrai que le décret présidentiel pourrait être annulé ou remplacé par la prochaine administration présidentielle faisant ainsi de lui un outil très politique. Le législateur fédéral des USA planche actuellement sur une législation fédérale en matière de protection des données (*American Data Privacy and Protection Act)*, dont les tenants et aboutissants sont résumés par le *Congressionnal Research Service*.

Du point de vue de la Suisse, un nombre important de questions demeure, en particulier s'agissant de savoir si notre pays peut être considéré comme un « *Qualifying State* ». Cela dit, si la Commission européenne venait à prendre une décision d'adéquation, il est probable que la Suisse lui emboîterait le pas, et déciderait à son tour d'adopter une décision d'adéquation (le cas échéant en y ajoutant un *Swiss finish*).

Proposition de citation : Jeremy Reichlin / Livio di Tria, Les transferts transatlantiques de données personnelles : *quo vadis* ?, 21 décembre 2022 *in* www.swissprivacy.law/192