DS AVOCATS

FLASH INFO

Privacy Shield : Le bouclier brisé par la CJUE

La saga judiciaire opposant Maximilian Schrems au géant Facebook prend fin après 8 ans de lutte procédurale. Dans une décision très attendue en date du 16 Juillet 2020, la CJUE annule le « bouclier de protection des données UE-Etats-Unis ». Néanmoins, la Cour valide les clauses contractuelles types relatives au transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers.

Pour rappel, suite à l'annulation du « *Safe Harbor* » par la CJUE dans un arrêt rendu le 06 Octobre 2015, Maximilian Schrems a déposé une plainte auprès de l'autorité irlandaise de contrôle, au motif que le successeur du *Safe Harbor*, le *Privacy Shield* (globalement approuvé par le G29 le 13 avril 2016, entérinée par la décision 2016/1250 de la Commission Européenne le 12 juillet 2016, en dépit toutefois de critiques persistantes du G29 devenu CEPD, rappelées en 2019) n'offrait pas de protection suffisante des données transférées vers les Etats-Unis. Le plaignant demandait par conséquent la suspension des transferts de ses données à caractère personnel depuis l'Union Européenne vers ce pays.

La Haute Cour irlandaise a donc interrogé la CJUE sur :

- L'application du RGPD aux transferts de données à caractère personnel fondés sur des clauses types de protection (« *standard contractual clauses* », qui assortissent de nombreux contrats prévoyant des flux transfrontaliers de données en dehors de l'UE) ;

- Le niveau de protection exigé par le RGPD dans le cadre d'un tel transfert ;

- Les obligations incombant aux autorités de contrôle en cas de transfert de données à caractère personnel vers un pays tiers ;

- La validité tant des décisions 2010/87 et 2016/1250 de la Commission Européenne qui avaient avalisé, les clauses contractuelles types, pour la première, et le *Privacy Shield,* pour la seconde.

La Cour rappelle dans un premier temps que le RGPD s'applique à un transfert de données à caractère personnel effectué à des fins commerciales par une entité exportatrice établie dans un État membre vers une entité destinataire établie dans un pays tiers, même si ces données sont susceptibles d'être traitées par la suite à des fins de sécurité publique par les autorités dudit pays tiers.

La CJUE rappelle notamment les dispositions du RGPD qui s'appliquent aux transferts, dont notamment les considérants 103 à 109. La CJUE vise également les articles du RGPD relatifs à l'encadrement des flux transfrontaliers de données, soit les articles 44 à 49, qui exposent notamment les différentes garanties juridiques et organisationnelles qu'il convient de mettre en œuvre pour permettre un tel flux, à défaut de quoi le transfert est tout simplement prohibé.

Le juge européen estime en outre que l'évaluation du niveau de protection doit prendre en compte les stipulations contractuelles convenues entre l'exportateur des données et le destinataire du transfert. À ce sujet, il précise qu'en matière de transfert de données à caractère personnel, les autorités de contrôle ont pour obligation de suspendre ou d'interdire un tel transfert dès lors qu'elles estiment, d'une part, que les clauses types de protection des données ne peuvent être respectées dans le pays tiers destinataire des données, et que, d'autre part, la protection des données transférées ne peut pas être assurée par d'autres moyens.

Le plaignant Maximilian Schrems avait initialement contesté la faculté pour Facebook, l'entité visée par sa démarche, d'envoyer ses données personnelles aux USA en s'appuyant sur le *Safe Harbor*. Après invalidation de celui-ci dans l'arrêt « *Schrems I* » du 6 octobre 2015, le plaignant avait reformulé sa plainte pour contester ensuite la faculté de Facebook de transférer ses données aux USA en s'appuyant désormais sur le *Privacy Shield* d'une part et les clauses contractuelles types d'autre part. La CJUE était donc invitée à se prononcer sur la

validité de ces deux décisions de la Commission européenne qui fondaient les transferts de données vers les USA.

Conformément aux articles 44 et suivants du RGPD, il s'agit là de deux types de « garanties » censées assurer un niveau de protection substantiellement équivalent à celui garanti au sein de l'UE par le RGPD.

Dans son examen de validité de la décision 2010/87, la CJUE estime que la décision impose tant à l'exportateur des données qu'au destinataire du transfert l'obligation de vérifier le respect d'un niveau de protection adéquat. Le fait qu'existent des réglementations nationales spécifiques dans le pays destinataire n'est pas, en soi, un facteur invalidant les clauses contractuelles types ; le cas échéant, le destinataire des données doit alors informer l'exportateur de son incapacité à se conformer aux clauses types de protection, et l'exportateur de données doit renoncer au transfert, ou rechercher un autre mécanisme.
Ainsi, **la CJUE estime que les clauses contractuelles types en matière de transfert de données vers des pays tiers sont valides, en ce qu'elles permettent d'assurer un niveau de protection adéquat au sens du RGPD**, et ce même si elles ne lient pas, en tant que telles, les autorités du pays destinataire.

Cela signifie que l'extension du niveau de protection adéquat hors d'UE est le fait de l'accord contractuel entre l'exportateur et l'importateur de données, via le mécanisme des clauses contractuelles types, et que ce mécanisme est pleinement reconnu et continue donc de s'appliquer à l'ensemble des transferts qu'il encadre. Il appartient simplement aux parties au transfert de s'assurer que ces clauses contractuelles types ne sont pas contredites, dans les faits, par la législation locale.

Tous les contrats entre entreprises européennes et destinataires extra-européens (partenaires commerciaux, prestataires sous-traitants) qui sont assortis des clauses contractuelles types conservent donc leur pleine validité sur ce point.

En revanche, s'agissant du Privacy Shield, la CJUE s'oppose à la décision 2016/1250 de la Commission, et la juge invalide.

La CJUE critique en effet le fait que, dans la décision 2016/1250, la Commission européenne avait reconnu la primauté des exigences relatives à la sécurité nationale, à l'intérêt public et au respect *de la législation américaine*, sur la stricte application de la réglementation européenne (incluant la protection des droits fondamentaux de la Charte des droits fondamentaux de l'UE).

Or, le fait que les USA veuillent imposer le respect de leur propre législation sécuritaire ne saurait écarter la pleine application du RGPD aux données des européens qui sont transférées vers le territoire nord-américain. Le transfert demeure, en toute hypothèse, un traitement de données personnelles au sens du RGPD.

Ainsi, comme la protection des données personnelles des européens doit être substantiellement la même sur le territoire nord-américain qu'au sein de l'UE, se posait la question de la compatibilité de la législation sécuritaire US avec ce niveau de protection.

Or, l'accès et l'utilisation par les autorités publiques nord-américaines des données personnelles transférées depuis l'Union est contraire au principe de proportionnalité exigé par le RGPD, les programmes de surveillance des autorités américaines ne se limitant pas au strict nécessaire.

La CJUE note à cet égard que selon la juridiction de renvoi, « *le droit de ce pays tiers* (les USA) *ne prévoit pas les limitations et les garanties nécessaires à l'égard des ingérences autorisées par sa réglementation nationale et n'assure pas non plus une protection juridictionnelle effective contre de telles ingérences. À ce dernier égard, elle ajoute que l'instauration du médiateur du bouclier de protection ne peut, selon elle, remédier à ces lacunes dès lors que ce médiateur ne saurait être assimilé à un tribunal, au sens de l'article 47 de la Charte* (des droits fondamentaux de l'UE) ».

La CJUE ajoute en effet que, si la réglementation américaine en matière de protection des données prévoit que les autorités doivent respecter ces exigences lors de la mise en œuvre des programmes de surveillance, elle ne confère pas aux personnes concernées des droits opposables aux autorités américaines devant les tribunaux, tel que l'exige le droit de l'Union – alors qu'il s'agit bien entendu d'une condition nécessaire pour considérer que les données personnelles sont aussi bien protégées aux USA qu'au sein de l'UE.

Autrement dit, le garde-fou mis en place dans le Privacy Shield ne constitue pas une voie de recours offrant des garanties substantiellement équivalentes à celles requises en droit de l'Union, dont l'exigence d'indépendance par rapport aux autorités américaines.

Une telle décision est une victoire (prévisible) pour les défenseurs des libertés. Toutefois, elle n'est pas sans conséquences : un vide juridique en matière de transfert de données vers des pays tiers a été créé, de nouveau. En effet, les Etats-Unis ne peuvent plus se prévaloir d'un niveau de protection adéquat dans le cadre d'un transfert de données à caractère personnel par une entreprise établie dans un Etat membre de l'Union, du fait de l'invalidation du programme précédemment reconnu comme tel. Cette annulation a donc pour effet d'entraîner un risque de commettre une infraction au RGPD pour l'ensemble des entreprises qui transfèrent leurs données vers les USA sur la seule base du *Privacy Shield*.

En l'état actuel des choses, l'établissement d'une convention de mise à disposition de données entre tiers semble être le choix le plus judicieux pour sécuriser un transfert de données vers un pays tiers, à condition toutefois de répondre aux exigences du RGPD. Comme on l'a vu, il est possible de recourir aux clauses contractuelles types, puisqu'elles sont confirmées. Des conventions de flux, qui ne modifient pas la teneur des clauses contractuelles types mais qui viennent ajouter des protections et donner effets aux droits

des personnes concernées nouvellement créés par le RGPD mais pas expressément visés dans les clauses contractuelles types de 2010, sont également préconisées.

Toutefois, cette mise à jour peut prendre du temps. Et dans cette attente, un certain nombre de flux sont désormais hors la loi. Comme en 2015 lors de l'annulation du *Safe Harbor*, certaines entreprises vont sans doute rapatrier leurs données en urgence vers des prestataires européens et des serveurs situés sur le territoire européen, seul moyen de faire échapper leurs données aux compétences exorbitantes et opaques des services secrets américains. Mais toutes n'ont pas cette latitude (on pense notamment aux grands « cloud provider » américains).

Il est dès lors conseillé aux clients de ces cloud providers notamment, de solliciter le plus rapidement possible, par la voie d'avenants, que leurs prestataires américains se conforment aux « clauses contractuelles types ». Plus nombreux seront les clients européens à faire cette démarche, moins les prestataires américains pourront s'y dérober.

Au-delà, cette décision, 5 ans après celle qui a sonné le glas du *Safe Harbor*, pose la question de l'hypocrisie qui caractérise certaines législations étrangères, et tout particulièrement les relations transatlantiques. Qu'un programme de ce type soit invalidé une fois, peut se comprendre compte tenu de la complexité des réglementations en Europe et aux USA ; mais deux fois ? Il ne faut pas s'illusionner : il s'agit là d'un nouvel épisode dans l'affrontement juridico-économique qui se poursuit entre les deux continents.