WilhelmGilliéron
AVOCATS

Auteur: Wilhelm Avocats | Le : 20 juillet 2020

Schrems II : le transfert des données personnelles aux Etats-Unis est-il encore permis ?

Dans une décision longuement attendue (C-311/18), rendue le 16 juillet 2020 et d'ores et déjà largement médiatisée, la Cour de Justice de l'Union Européenne était amenée à se prononcer sur la validité des clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers (Décision 2010/87, telle que modifiée par la Décision 2016/2297, plus communément appelées « clauses modèles »), respectivement sur celle du bouclier de protection des données UE-Etats Unis (Décision 2016/1250, plus communément désigné sous le terme anglais « *Privacy Shield* »).

Si les clauses modèles ont été sauvées de justesse, cet arrêt sonne en revanche le glas du « *Privacy Shield* ».

I. Rappel des principes sous-jacents au transfert des données vers un Etat tiers

A titre liminaire, il est bon de rappeler que le transfert des données émanant d'un Etat membre de l'UE vers un pays tiers exige soit que le pays destinataire ait été reconnu par la Commission comme offrant un niveau de protection considéré comme étant adéquat (art. 45 RGPD ; pour une liste de ces pays, dont la Suisse fait à ce jour partie, voir ici), soit que le responsable du traitement ait prévu des garanties appropriées (art. 46 RGPD).

En sus des clauses modèles, expressément admises comme une forme de garantie appropriée permettant le transfert vers les Etats-Unis (art. 46 al. 2 lit. c RGPD), les Etats-Unis étaient jusqu'alors reconnus comme offrant un niveau de protection adéquat en ce qui avait trait aux entreprises ayant décidé de se soumettre volontairement au « *Privacy Shield* » (pour une liste de ces entreprises, voir ici).

II. Rappel des faits ayant conduit au litige

En substance, Maximillian Schrems, un ressortissant autrichien, faisait valoir que le transfert de ses données à caractère personnel par Facebook Ireland à Facebook Inc. aux Etats-Unis n'offrait pas les garanties d'assurance nécessaires en tant que la législation américaine en matière de surveillance violait les art. 7 (droit au respect de la vie privée et familiale), 8 (protection des données à caractère personnel) et 47 (droit à un recours effectif et à accéder à un tribunal impartial) de la Charte des droits fondamentaux de l'Union Européenne.

En cause, deux actes particuliers : tout d'abord, l'art. 702 FISA (*Foreign Intelligence Surveillance Act*), aux termes duquel les procureur général et directeur du renseignement national peuvent conjointement autoriser la surveillance de ressortissants non américains se trouvant en dehors du territoire américain pour se procurer des « informations en matière de renseignement extérieur » ; cette disposition sert de base aux programmes de surveillances PRISM (lequel permet d'enjoindre les fournisseurs de services Internet à fournir à la NSA, et dans une certaine mesure au FBI et à la CIA toutes les communications envoyées et reçues par un individu

déterminé) et UPSTREAM (lequel permet d'enjoindre les entreprises de télécommunication exploitant la « dorsale » de l'Internet d'autoriser la NSA à copier et filtrer les flux de trafic Internet pour recueillir les communications envoyées par ou reçues par le ressortissant non américain déterminé). Ensuite, l'E.O. 12333, qui permet à la NSA d'accéder à des données « en transit » vers les Etats-Unis, en accédant aux câbles sous-marins posés sur le plancher de l'Atlantique, ainsi que de recueillir et conserver ses données avant qu'elles n'arrivent aux Etats-Unis et y soient soumises au FISA.

III. La validité des clauses modèles

A titre liminaire, la Cour devait se prononcer sur la question de savoir si un traitement de données opéré pour des raisons de sécurité n'était pas exclu du champ d'application du RGPD, plus particulièrement au regard de son art. 2.2 lit. a, dont l'interprétation exclut notamment l'application du RGPD lorsque le traitement des données a lieu par des autorités pour des raisons de sécurité nationale. La Cour répond par la négative, en estimant que ce n'est pas le traitement éventuel par les autorités américaines qui est ici en cause, mais bien le transfert entre deux entités économiques (à savoir Facebook Ireland d'un côté, et Facebook Inc. de l'autre). Or, la possibilité que les données à caractère personnel transférées entre deux opérateurs économiques à des fins commerciales subissent, au cours ou à la suite de ce transfert, un traitement à des fins de sécurité publique n'a pas pour effet de soustraire ce transfert du champ d'application du RGPD.

Cette question liminaire étant réglée, la Cour se penche sur la question de savoir si les clauses modèles peuvent être considérées comme une « garantie appropriée » permettant le transfert aux Etats-Unis comme le prévoit l'art. 46 RGPD. En substance, son raisonnement est le suivant :

- La question de savoir s'il existe des « garanties appropriées » et la mise à disposition de « droits opposables et de voies de droit effectives » comme l'exige l'art. 46.1 RGPD doit être examinée à la lumière des droits fondamentaux garantis par la Charte, laquelle constitue le référentiel de base pour juger de l'adéquation d'un pays au regard de l'art. 45 RGPD.

- Dans ce cadre, si le contenu des clauses modèles peut constituer des « garanties appropriées », encore faut-il que le responsable du traitement s'assure que les possibilités d'accès aux données par les autorités publiques du pays destinataire et moyens mis à disposition des individus concernés puisse être considéré comme étant acceptable, une question qui sera examinée à l'aune des critères posés par l'art. 45.2 RGPD.

- Le fait pour la Commission d'avoir adopté des clauses modèles comme le lui permet l'art. 46.2 lit. c RGPD ne soustrait pas pour autant l'examen de ces clauses par l'autorité de contrôle et la possibilité pour cette autorité de prendre le cas échéant les mesures prévues par l' 58.2 lit f et j RGPD. Il faut toutefois alors distinguer suivant que le pays destinataire a fait l'objet d'une décision d'adéquation au sens de l'art. 45.1 RGPD ou non.

- Lorsque le pays destinataire a été reconnu comme proposant un niveau de protection adéquat au sens de l'art. 45.1 RGPD (hypothèse dans laquelle on peine à dire vrai à voir l'intérêt de recourir aux clauses modèles), une autorité de contrôle ne peut pas de son propre chef adopter de mesures contraires à une telle décision d'adéquation ; toutefois, cette décision n'empêche pas un individu dont les données auraient été transférées de former réclamation en violation de ses droits fondamentaux auprès de l'autorité nationale de contrôle compétent, comme le lui permet l' 77 RGPD.

- Ainsi saisie par un particulier, l'autorité de contrôle doit pouvoir examiner en toute indépendance si le transfert opéré respecte les exigences posées par le RGPD quitte, si nécessaire, à introduire un recours devant les juridictions nationales pour que ces dernières procèdent, le cas échéant, à un renvoi préjudiciel devant la Cour aux fins de l'examen de cette validité. Ce n'est toutefois qu'une fois la décision invalidée par la Cour que l'autorité de contrôle peut ensuite suspendre ou interdire le transfert de données vers le pays en question en application de l'art. 58 RGPD précité.

- Lorsque le pays destinataire ne bénéficie pas d'une telle décision d'adéquation, la réponse est toutefois différente. La Cour rappelle que, certes, les clauses modèles ne lient que les parties, à l'exclusion des autorités du pays destinataire qui ne sont évidemment pas partie au contrat. Le fait que les autorités ne soient pas liées ne signifie cependant pas pour autant que ces clauses sont invalides. En revanche, à partir du moment où la teneur de ces clauses est standard et que, à ce titre, elle ne tient pas nécessairement compte de la législation du pays destinataire, notamment quant à ses possibilités d'ingérence, il incombe au responsable du traitement de procéder à une analyse de la réglementation applicable pour, si

besoin, est, compléter ces clauses modèles sur un point ou l'autre.

Autrement dit, incorporer une clause modèle ne suffit pas à garantir que le transfert présente les garanties adéquates. Encore faut-il que la législation du pays destinataire offre des moyens effectifs aux individus pour se plaindre d'une éventuelle violation de leurs droits en application de l'art. 47 de la Charte. Si tel n'est pas le cas, le recours aux clauses modèles sans complément quel qu'il soit doit alors être considéré comme insuffisant. En cette hypothèse, l'autorité de contrôle peut alors directement intervenir sur la base de l'art. 58 RGPD précité pour suspendre ou interdire le transfert.

L'art. 4 lit. a de la clause modèle impose en effet au responsable de s'assurer que la législation du pays tiers permet au destinataire de se conformer aux obligations contenues dans la clause modèle. L'art. 5 lit.a de la clause modèle apporte cependant dans ce cadre une aide bienvenue au responsable de traitement, puisque l'importateur se doit de l'informer dans les meilleurs délais de son éventuelle incapacité à se conformer à ses obligations contenues dans dite clause, l'art. 5 lit. b renforçant cette obligation, en prévoyant que l'importateur confirme de surcroît n'avoir aucune raison de croire que la législation applicable l'empêche de ses conformer à ces obligations.

A supposer en revanche que l'importateur ne puisse se conformer à ses obligations, la Cour considère que l'art. 4 lit. a de la clause modèle impose alors au responsable de traitement de suspendre ou interdire tout transfert, étant précisé que l'art. 12 exige en sus que les données déjà transférées soient restituées ou détruites. A supposer que la législation change, ce dont l'importateur devrait informer le responsable du traitement, il est loisible au responsable de décider de poursuivre le traitement, mais il doit alors en informer l'autorité de contrôle, conformément à l'art. 4 lit. g de la clause modèle. Là encore, il sera alors loisible à l'autorité de contrôle de suspendre ou interdire tout traitement, conformément à l'art. 58 RGPD.

Au vu du système ainsi mis en place par le jeu des art. 4 et 5 de la clause modèle, la Cour considère que celle-ci prévoit des moyens effectifs répondant aux exigences des art. 7, 8 et 47 de la Charte. Ce faisant, la Cour confirme par là-même la validité de principe des clauses modèles.

IV. L'absence d'adéquation du Privacy Shield

Si le jeu des art. 4 et 5 de la clause modèle en sauve la validité, un tel mécanisme n'est en revanche pas prévu par le *Privacy Shield*. Pour la Cour, le *Privacy Shield* n'offre pas les garanties appropriées de protection à deux égards :

- Le point 1.5 de l'Annexe II retient expressément que l'adhésion aux principes peut être limitée par, notamment, « les exigences relatives à la sécurité nationale, [à] l'intérêt public et [au] respect de la législation ». Cette primauté de l'ingérence étatique sur les droits fondamentaux n'est pas contrebalancée par quelque limite que ce soit qui serait contenue dans le cadre des programmes de surveillance PRISM et UPSTREAM fondés sur l'article 702 du FISA, ainsi que sur le fondement de l'E.O. 12333. Ce faisant, le droit américain contrevient aux principes de nécessité et de proportionnalité et, plus largement, aux art. 7, 8 et 52 de la Charte dont il ressort que toute ingérence dans les droits fondamentaux doit être subordonnée à une définition quant à la portée de la limitation de l'exercice du droit concerné, prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposer des exigences minimales.

- La mise sur pied d'un médiateur, prévue à l'Annexe III, ne peut être considérée comme un moyen effectif permettant un contrôle judiciaire au sens de l'art. 47 de la Charte, dès lors que ce médiateur rend directement compte au secrétaire d'Etat et qu'il fait partie intégrante du département d'Etat des Etats-Unis, sans qu'aucune voie de recours devant un organe offrant des garanties comparables à celles prévues par l'art. 47 de la Charte ne soit prévue.

Au vu de ce qui précède la Cour prononce l'invalidité de la Décision 2016/1250.

V. Implications pratiques

Que penser au final de cet arrêt ?

- Tout d'abord, il convient de rappeler que les entreprises ayant adhéré au *Privacy Shield*, nonobstant l'invalidation de la Décision 2016/1250, continuent à y être soumis et, à ce titre, doivent continuer à satisfaire à leurs obligations en résultant. On peut toutefois douter de l'intérêt que ces entreprises auront à continuer à y être soumis, puisque l'objectif principal poursuivi par cette adhésion est désormais sans objet. Partant, on peut penser qu'elles préféreront entamer un processus de retrait. L'avenir le dira.

- Ensuite, l'arrêt rendu repose essentiellement sur un examen de la compatibilité des décisions attaquées avec la Charte des droits fondamentaux de l'Union Européenne, laquelle n'est pas applicable à la Suisse. En déduire que l'arrêt n'aura pas d'incidence en Suisse serait cependant bien naïf. Bien que le Préposé fédéral ne se soit pour le moment pas encore formellement prononcé sur l'impact de cet arrêt quant à la validité du *Privacy Shield* Suisse-Etats-Unis, on peut difficilement imaginer qu'il prenne une position différente au regard de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (plus communément appelée Convention 108). Les entreprises suisses dont les activités impliquent un traitement aux Etats-Unis auront donc tout intérêt à considérer la situation à l'image de n'importe quelle entreprise sise au sein de l'Union Européenne.

A cet égard, on relèvera les étapes d'analyse suivantes :

- Un premier lot d'entreprises, généralement de taille déjà importante, doublaient déjà leur adhésion au *Privacy Shield* à la conclusion de clauses modèles. Pour celles-ci, l'urgence apparaît moindre.

- Un second lot, ayant anticipé la possible invalidation du *Privacy Shield*, avait expressément prévu qu'en cette hypothèse, les parties recourraient à une clause modèle. Pour ces entreprises, il s'agit donc de se mettre désormais en contact et signer une telle clause.

- Un troisième lot, d'ores et déjà dubitatif quant à la validité du *Privacy Shield*, avait décidé de recourir d'emblée aux seules clauses modèles.

- Le fait d'être au bénéfice d'une clause modèle, existante ou à venir, ne suffit plus. Chaque responsable de traitement, aidé en cela par l'importateur, devra s'assurer que la législation existante permet à l'importateur de se conformer à ses obligations et offre aux sujets traités des moyens effectifs de se plaindre d'éventuelles violation de leurs droits fondamentaux.

S'agissant du transfert vers les Etats-Unis, on peine à avoir comment la législation pourrait consacrer des moyens effectifs au regard de l'art. 47 de la Charte lorsque le responsable du traitement recourt à une clause modèle, alors que cette disposition serait violée au regard du *Privacy Shield*. Sauf à anonymiser les données, le transfert des données aux Etats-Unis risque donc désormais de donner du fil à retordre aux acteurs du marché, sauf à vouloir accepter la prise de risque en résultant. Une analyse serrée sera donc ici nécessaire.

Cela étant, cette approche vaut non seulement pour les Etats-Unis, mais pour tous les pays n'offrant pas un niveau adéquat de protection, soit en réalité une très large majorité d'Etats. Ainsi le responsable du traitement devra-t-il apprécier les risques en s'interrogeant en particulier sur : (i) l'étendue du traitement, (ii) la manière dont les données sont traitées, (iii) les pouvoirs des autorités susceptibles de vouloir accéder aux données, et (iv) la possibilité de s'opposer à une telle requête (le cas échéant en justice).

A supposer que cette évaluation des risques aboutisse à la conclusion que la législation en cause n'offre pas les garanties suffisantes, le responsable du traitement devrait alors s'efforcer de compléter les clauses modèles pour remédier à ces lacunes à lire la Cour.

Force est d'admettre que l'on peine toutefois à voir de quelle manière des insuffisances législatives pourraient, par la voie contractuelle, permettre de remédier à une ingérence étatique…Sans doute des clauses plus précises et obligations supplémentaires mises à la charge de l'importateur seront-elles à tout le moins susceptibles de témoigner des efforts mis en œuvre par le responsable du traitement pour déceler les problèmes et y remédier, et ainsi réduire les conséquences néfastes que toute absence d'évaluation pourrait faire peser sur lui. Le Comité européen de la protection des données devrait fournir certaines lignes directrices en la matière dans un proche avenir.

Au final, se lancer dans une telle évaluation des risques semble toutefois être l'apanage des plus gros acteurs du marché. A certains égards compréhensibles, les arguments avancés omettent toutefois de prendre en considération la réalité économique et les coûts faramineux auxquels une évaluation systématique des risques pour tout pays n'offrant pas un niveau de protection adéquat aboutira pour la très grande majorité des entreprises, puisqu'il s'agit en effet d'une très large majorité de pays en dehors de l'UE. Les prestataires des pays « tiers » seront-ils d'accord d'avaler les coûts de cette analyse que les responsables de traitement les inviteront bien souvent à mener pour leur offrir les garanties nécessaires, respectivement les intégrer sur le plan commercial dans leur modèle de prix ?

A supposer qu'une telle évaluation soit systématiquement nécessaire comme nous y conduit le raisonnement de la Cour, une telle charge ne contrevient-elle pas au but même de la clause modèle et la facilité d'exécution recherchée visant à se dispenser de l'accord préalable de l'autorité de contrôle ? Qui dit évaluation des risques ne dit-elle pas également obligation de les documenter ? En ce cas, ne vaudrait-il pas alors plutôt favoriser un accord préalable de l'autorité de contrôle, une démarche que les clauses modèles avait justement pour but d'éviter ?

Certes, les temps ont changé depuis l'adoption des clauses modèles, et les ingérences prises au regard de la sécurité nationale sont, pour beaucoup d'Etats, un moyen propice à une surveillance excessive. Dans ses effets, l'arrêt de la Cour est ainsi susceptible de favoriser un re-cloisonnement des marchés, une vision certes possible, mais cependant encore bien loin de la réalité d'une économique qui est, et demeurera assurément pour longtemps à la supposer jamais remise en cause, largement mondialisée. Est-ce à dire que cet arrêt demeurera largement impraticable sauf à réviser les clauses modèles pour les mettre au goût du jour ? C'est à voir.

En toute hypothèse, au vu de ce qui précède, sauf à pouvoir totalement anonymiser les données traitées, une tâche toujours plus difficile, il apparaît raisonnable de penser que la très grande majorité des acteurs du marché préférera pour le moment adhérer aux clauses modèles sans plus ample analyse et prendre les risques en découlant plutôt que de se lancer systématiquement dans une telle analyse. Cette position risque en tous les cas de prévaloir aussi longtemps que le Comité européen de la protection des données et les autorités de contrôle ne se seront pas concertés pour émettre des lignes directrices quant à la manière dont cet arrêt va désormais être appliqué en pratique.

Gageons que l'attitude des autorités de contrôle sera ici comme ailleurs un vecteur quant à l'attitude à adopter : si l'ICO semble d'ores et déjà désireux de faire preuve d'un certain pragmatisme, il n'en va pas de même à Berlin, où le Préposé a informé que les responsables de traitement devaient dès maintenant se conformer à l'arrêt et rechercher, notamment s'agissant au recours à des prestataires cloud, des alternatives permettant un rapatriement des données en Europe.

Dans un prochain article, nous examinerons la manière dont les transferts aux Etats-Unis peuvent, potentiellement, avoir lieu.

Source : https://www.wg-avocats.ch/actualites/schrems-transfert-donnees-usa/