PROTECTION DES DONNÉES. Depuis la décision de la CJUE du 16 juillet, il est interdit aux entreprises de l'Union européenne de transférer de données à caractère personnel sur la base du *Privacy Shield* à destination d'entreprises américaines. La décision impacte également les transferts de données vers les autres pays tiers de l'UE. Devant le silence de la CNIL, nous faisons le point sur les mesures que doivent prendre les entreprises pour éviter d'être sanctionnées.

Invalidation du « Privacy Shield » : conséquences pratiques

Entretien avec
Ariane Mole
Avocate associée
cabinet Bird & Bird

Semaine sociale Lamy : *La CJUE a, dans un arrêt du 16 juillet 2020, invalidé le* Privacy Shield. *De quoi s'agit-il ?*

Ariane Mole : Le *Privacy Shield* était l'accord international qui régissait les transferts de données personnelles depuis l'Union européenne vers les États-Unis. Pour rappel, conformément au RGPD (Règlement européen pour la protection des données) les entreprises européennes n'ont pas le droit de transférer des données à caractère personnel hors de l'UE, par exemple sur leurs clients ou sur leurs salariés, sauf s'il existe des garanties spécifiques permettant d'assurer la protection de ces données dans le pays destinataire. Les transferts vers les États-Unis pouvaient reposer sur un mécanisme de certification des entreprises américaines, le *Privacy Shield*. Une autre possibilité, utilisée par de nombreuses entreprises en Europe, consiste à encadrer les transferts au moyen de contrats spécifiques fondés sur des clauses contractuelles type (CCT) dont le texte a été établi par la Commission européenne. C'est la validité de ces deux mécanismes qui était contestée devant la Cour de Justice de l'Union européenne.

Quels sont les faits ?

A. M. : L'affaire est également connue sous le nom de Schrems II. Max Schrems, qui est un citoyen autrichien, avait déjà obtenu en 2015 l'annulation par la CJUE du *Safe Harbor* qui était l'accord international qui précédait le *Privacy Shield*. Plus précisément, Max Schrems, en tant qu'utilisateur de Facebook, contestait la validité des transferts de ses données par Facebook vers les serveurs de Facebook Inc. situés aux Etats-Unis car il estimait que la législation américaine n'offrait pas une protection suffisante des données personnelles des citoyens européens hébergées aux Etats-Unis. En effet, dans le cadre des programmes de surveillance de masse, la réglementation américaine (*Foreign Intelligence Surveillance Act* – FISA, et décret présidentiel EO-12333) permet à des autorités publiques (FBI, NSA, CIA) d'accéder aux données personnelles transférées vers les Etats-Unis. Après l'invalidation du *Safe Harbor* en 2015, un nouvel accord avait ensuite été négocié, le *Privacy Shield*, et la Commission européenne avait estimé dans une décision du 12 juillet 2016 qu'il était de nature à assurer un niveau de protection des données à caractère personnel « *essentiellement équivalent* » aux exigences européennes. Max Schrems, dans sa nouvelle plainte, avait maintenu son argumentation selon laquelle la législation américaine n'offre toujours pas une protection suffisante des données à caractère personnel transférées vers ce pays. Comme Facebook fonde le transfert d'une grande partie des données sur le fondement des clauses contractuelles types (CCT), une demande d'annulation de ces clauses était également formulée.

Que dit la CJUE ?

A. M. : La CJUE a annulé le *Privacy Shield*, comme elle avait annulé le *Safe Harbor* en 2015. Elle considère qu'il n'y a pas d'adéquation car les États-Unis ne disposent pas d'une législation qui limite l'accès aux données à caractère personnel par les services de sécurité américains. En particulier, les résidents de l'UE dont les données sont transférées ne disposent pas de droits opposables aux autorités américaines devant les tribunaux. Cette décision est à effet immédiat, ce qui veut dire que depuis le 16 juillet, les transferts de données à caractère personnel sur la base du *Privacy Shield* à destination d'entreprises américaines sont illégaux. Et nous ne nous attendons pas à un nouvel accord avec les États-Unis dans un avenir proche.
En ce qui concerne les clauses contractuelles types, la Cour ne les a pas invalidées mais elle considère qu'elles ne sont pas suffisantes pour garantir la sécurité des données transférées vers un pays tiers hors de l'UE. Les entreprises qui transfèrent des données sur la base de ces clauses doivent donc désormais procéder à une évaluation pour s'assurer que le pays importateur offre un niveau de protection suffisant, c'est-à-dire qu'il a mis en place une législation qui permet d'assurer des garanties et qui limite l'accès aux données par ses autorités de surveillance. À défaut, l'entreprise (responsable de traitement ou sous-traitant dans l'UE) doit prendre des mesures supplémentaires pour compenser l'absence de garanties offertes par la législation du pays destinataire. Mais la CJUE n'a

pas indiqué quelles pourraient être ces mesures et c'est un des problèmes. C'est donc une charge et une responsabilité supplémentaires pour les entreprises qui jusqu'ici se contentaient de signer avec l'entreprise hors UE un contrat de transfert reprenant le texte des CCT dans lequel cette dernière s'engageait à respecter le RGPD.

Que doivent faire les entreprises concernées ?

A. M. : Si ce n'est pas déjà fait depuis le 16 juillet 2020, l'entreprise doit tout d'abord recenser tous ses transferts de données, à destination de pays tiers à l'UE, et en particulier à destination des États-Unis. Elle peut s'appuyer sur son registre des traitements à condition qu'il soit à jour. Lorsque les données sont transférées sur la base du *Privacy Shield*, un tel transfert est désormais interdit, donc l'entreprise doit, comme le prévoit la CJUE, soit trouver une autre base juridique, soit mettre fin au transfert. C'est évidemment plus facile à dire qu'à faire. L'entreprise ne pourra pas non plus – contrairement à ce qui s'était passé en 2015 suite à l'annulation du *Safe Harbor* – simplement remplacer le *Privacy Shield* par la signature de contrats de transferts fondés sur les CCT puisque la CJUE vient précisément de juger que les CCT n'assurent pas une protection suffisante pour un transfert vers les États-Unis. S'agissant de transferts de données concernant les salariés, les autorités de protection des données personnelles considèrent que ceux-ci ne peuvent pas non plus être fondés sur le consentement du salarié. On peut imaginer que par exception, certains transferts soient possibles sur la base du consentement, par exemple lorsqu'ils sont clairement nécessaires à la bonne exécution du contrat avec le salarié. C'est le cas, par exemple, pour les salariés expatriés. Dans les autres cas, certaines autorités de protection des données personnelles, notamment en Allemagne, ont suggéré la mise en place de mesures techniques (comme par exemple le cryptage) pour empêcher que les données transférées puissent être lues par les autorités publiques de surveillance. De manière générale, plusieurs entreprises sont amenées à vérifier comment réduire ou supprimer certains transferts non essentiels à leur activité.

Quid *des transferts vers les autres pays tiers ?*

Lorsque les données sont transférées vers un autre pays tiers à l'UE, sur le fondement de clauses contractuelles types, l'entreprise doit procéder à une évaluation des transferts envisagés et à une étude d'impact. Cela implique :
– de prendre en compte la nature (la sensibilité) des données transmises, à qui, sous quelle forme ;
– de déterminer si le pays vers lequel les données sont transférées est reconnu comme bénéficiant d'un niveau de protection adéquat ; l'entreprise doit procéder à une évaluation de la législation du pays importateur de données et des risques encourus en cas de transfert (par exemple vérifier si dans le passé les données ont fait l'objet de demandes de communication de la part des autorités de surveillance dans le pays de destination, si la nature des données transférées est susceptible d'intéresser une autorité de surveillance, etc.) ;
– de déterminer s'il est possible de crypter ou de pseudonymiser les données transférées.

Le cas échéant, que risque l'entreprise ?

A. M. : En cas de transfert non autorisé, le RGPD prévoit une amende administrative pouvant aller jusqu'à 20 000 000 euros ou 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu *(RGPD, art. 83)*. Cette amende peut être imposée par la CNIL comme par ses homologues au sein de l'UE. À ce jour, la CNIL n'a prononcé aucune sanction – il est trop tôt - mais des plaintes ont été déposées. Depuis le 16 juillet 2020, Max Schrems a déposé 101 plaintes auprès des autorités européennes de protection des données personnelles, y compris auprès de la CNIL, *via* son association NOYB (*None Of Your Business*). Sont visées des entreprises européennes qui utilisent les services de Facebook ou de Google et qui fondent leurs transferts de données vers les USA sur des clauses contractuelles types ou sur le *Privacy Shield*. Mais d'autres plaintes sont probablement à venir, qui vont concerner des transferts vers les États-Unis vers d'autres entreprises que Facebook ou Google, ou des transferts vers d'autres pays tiers.

Quelles issues ?

A. M. : Les autorités de contrôle réfléchissent encore aux conséquences de la décision de la CJUE mais les entreprises ont un besoin urgent de lignes directrices, car elles ne disposent juridiquement d'aucun délai pour appliquer la décision : à ce jour, la CNIL diffuse sur son site internet le communiqué du Comité européen de la protection des données qui reprend les grandes lignes de l'arrêt de la CJUE et indique que les organismes sont tenus de mettre fin aux transferts de données vers les pays tiers qui n'assurent pas un niveau suffisant de protection, à moins de pouvoir mettre en place des mesures complémentaires, sans indiquer quelles pourraient être ces mesures. Nous savons que la Commission européenne a prévu de publier, d'ici fin décembre 2020, de nouveaux modèles de clauses contractuelles types qui rendront obligatoires les évaluations. Elle attendait pour ce faire la décision de la CJUE. Mais les nouvelles CCT ne résoudront pas le problème de fond.
On peut imaginer que, comme elles l'ont fait pour les traitements à risques qui doivent faire l'objet d'une étude d'impact en vertu du RGPD, les autorités de protection des données personnelles puissent élaborer une liste des pays à risques devant faire l'objet d'une évaluation spécifique. Il serait utile également que la CNIL fixe la liste des mesures techniques et juridiques qu'une entreprise peut prendre pour protéger ses données en cas de transfert vers un pays tiers. À défaut, tout repose sur les entreprises, déjà fortement impactées économiquement par le contexte sanitaire que nous connaissons. ■

Propos recueillis par Sabine Izard