Translations proofread by EDPB Members.

This language version has not yet been proofread.

Foire aux questions sur l'arrêt rendu par la Cour de justice de l'Union européenne dans l'affaire C-311/18 - *Data Protection Commissioner contre Facebook Ireland Ltd et Maximillian Schrems*

Adopté le 23 juillet 2020

L'objectif de ce document consiste à fournir des réponses à plusieurs questions fréquemment posées aux autorités de contrôle; ces questions seront développées et complétées par des analyses plus approfondies, étant donné que le comité européen de la protection des données continue d'examiner et d'évaluer l'arrêt rendu par la Cour de justice de l'Union européenne (la «Cour»).

L'arrêt C-311/18 est disponible ici, et le communiqué de presse de la Cour est disponible ici.

1) Qu'a décidé la Cour dans le cadre de son arrêt?

➔ Dans le cadre de son arrêt, la Cour a examiné la validité de la décision 2010/87/CE de la Commission européenne relative aux clauses contractuelles types et a considéré que cette dernière est valide. En effet, la validité de cette décision n'est pas remise en cause par le seul fait que les clauses types de protection des données de cette décision, compte tenu de leur nature contractuelle, ne lient pas les autorités des pays tiers vers lesquels des données à caractère personnel sont susceptibles d'être transférées.

Toutefois, comme l'a ajouté la Cour, ladite validité dépend du point de savoir si la décision 2010/87/CE comporte des mécanismes effectifs permettant, en pratique, d'assurer la conformité au niveau de protection substantiellement équivalent au niveau de protection garanti au sein de l'UE par le RGPD, et si les transferts de données à caractère personnel, fondés sur de telles clauses, sont suspendus ou interdits en cas de violation de ces clauses ou d'impossibilité de les honorer.

À cet égard, la Cour souligne notamment que la décision 2010/87/CE impose à l'exportateur de données et au destinataire de données (l'«importateur de données») de vérifier, préalablement à tout transfert, et en fonction des circonstances du transfert, que le niveau de protection est respecté par le pays tiers concerné, et souligne que la décision 2010/87/CE impose à l'importateur de données d'informer l'exportateur de données de son éventuelle incapacité de se conformer aux clauses types de protection, et, le cas échéant, à toute mesure supplémentaire aux dispositions établies par ces clauses, auquel cas l'exportateur de données serait, pour sa part, dans l'obligation de suspendre le transfert des données et/ou de mettre fin au contrat établi avec l'importateur de données.

➔ La Cour a également examiné la validité de la décision «bouclier de protection des données» (décision 2016/1250 relative à l'adéquation de la protection fournie par le Privacy Shield UE-États-Unis), puisque les transferts en question dans le contexte du litige national ayant conduit à la demande d'une décision préjudicielle ont été réalisés entre l'UE et les États-Unis.

La Cour a considéré que les exigences de la législation nationale des États-Unis, et notamment certains programmes autorisant les organismes du secteur public d'accéder à des données à caractère personnel transférées de l'UE vers les États-Unis à des fins de sécurité nationale, entraînent des restrictions en matière de protection des données à caractère personnel qui ne sont pas circonscrites de manière à être conformes aux exigences substantiellement équivalentes aux exigences requises en vertu du droit de l'Union[1], et que cette législation ne confère aux personnes concernées aucun droit d'action devant les tribunaux contre les autorités américaines.

En conséquence d'un tel degré d'interférence avec les droits fondamentaux des personnes dont les données sont transférées vers ce pays tiers, la Cour a invalidé la décision d'adéquation du bouclier de protection des données.

2) L'arrêt de la Cour a-t-il des conséquences sur les outils de transfert autres que le bouclier de protection des données?

➔ En règle générale, pour les pays tiers, le seuil établi par la Cour s'applique également à toutes les garanties appropriées au titre de l'article 46 du RGPD utilisées pour le transfert de données depuis l'EEE vers un pays tiers. Le droit des États-Unis mentionné par la Cour (par ex., la section 702 du FISA et l'EO 12333) s'applique à tous les transferts effectués vers les États-Unis par voie électronique et qui relèvent du champ d'application de cette législation, indépendamment de l'outil de transfert utilisé pour le transfert[2].

3) Existe-t-il une période de grâce pendant laquelle je peux continuer à transférer des données vers les États-Unis sans avoir à évaluer ma base juridique du transfert?

➔ Non, la Cour a invalidé la décision «bouclier de protection des données» sans en maintenir les effets, car le droit américain évalué par la Cour ne fournit pas un niveau de protection

[1] La Cour souligne que certains programmes de surveillance autorisant les organismes du secteur public à accéder à des données à caractère personnel transférées de l'UE vers les États-Unis à des fins de sécurité nationale ne prévoient aucune restriction du pouvoir conféré aux autorités des États-Unis ni l'existence de garanties pour les personnes non ressortissantes des États-Unis éventuellement ciblées.

[2] La section 702 du FISA s'applique à tous les «prestataires de services de communication électronique» [voir la définition établie au paragraphe 1881, point b), alinéa 4), du Titre 50 du Code des États-Unis], et l'EO 12333 définit la surveillance électronique comme «l'acquisition d'une communication non publique par des moyens électroniques sans le consentement d'une personne étant partie à une communication électronique ou, dans le cas d'une communication non électronique, sans le consentement d'une personne visiblement présente sur le lieu de la communication, mais à l'exclusion de l'utilisation d'un équipement radio de goniométrie uniquement pour déterminer l'emplacement d'un émetteur» [paragraphe 3.4, point b)].

substantiellement équivalent à celui de l'UE. Cette évaluation doit être prise en compte pour tout transfert effectué vers les États-Unis.

4) Je transférais des données à un importateur de données ressortissant des États-Unis adhérant au «bouclier de protection des données». Que dois-je faire à présent?

➔ Les transferts effectués sur la base de ce cadre juridique sont illégaux. Si vous souhaitez continuer à transférer des données vers les États-Unis, vous devez vérifier que vous êtes en mesure de le faire conformément aux conditions énoncées ci-dessous.

5) J'utilise des clauses contractuelles types avec un importateur de données basé aux États-Unis. Que dois-je faire?

➔ La Cour a conclu que le droit des États-Unis (c.-à-d. l'article 702 du FISA et l'EO 12333) ne garantit pas un niveau de protection substantiellement équivalent.

La possibilité de transférer ou non des données à caractère personnel sur la base de clauses contractuelles types dépendra du résultat de votre évaluation, en tenant compte des circonstances des transferts, et des mesures supplémentaires que vous pourriez mettre en place. Les mesures supplémentaires ainsi que les clauses contractuelles types émergeant d'une analyse au cas par cas des circonstances relatives au transfert doivent assurer que le droit des États-Unis n'affecte pas le niveau de protection adéquat qu'elles garantissent.

Si vous en arrivez à la conclusion que, compte tenu des circonstances du transfert et des éventuelles mesures supplémentaires, les garanties appropriées ne seraient pas garanties, vous êtes tenu de suspendre ou de mettre fin au transfert de données à caractère personnel. Toutefois, si vous avez l'intention de continuer à transférer des données malgré cette conclusion, vous devez en informer l'autorité de contrôle dont vous relevez[3].

6) J'utilise des règles d'entreprise contraignantes («BCR») avec une entité basée aux États-Unis. Que dois-je faire?

➔ Compte tenu de l'arrêt rendu par la Cour, qui a invalidé le «bouclier de protection des données» en raison du degré d'interférence créé entre le droit des États-Unis et les droits fondamentaux des personnes dont les données sont transférées vers ce pays tiers, et du fait que le «bouclier de protection des données» a également été élaboré dans l'objectif d'apporter des garanties aux données transférées avec d'autres outils comme les BCR, l'évaluation de la Cour s'applique également dans le contexte des BCR, puisque le droit des États-Unis primera également sur cet outil.

La possibilité de transférer ou non des données à caractère personnel sur la base de BCR dépendra du résultat de votre évaluation, en tenant compte des circonstances des transferts, et des mesures supplémentaires que vous pourriez mettre en place. Ces mesures supplémentaires ainsi que les BCR émergeant d'une analyse au cas par cas des circonstances relatives au transfert, doivent assurer que le droit des États-Unis n'affecte pas le niveau de protection adéquat qu'elles garantissent.

Si vous en arrivez à la conclusion que, compte tenu des circonstances du transfert et des éventuelles mesures supplémentaires, les garanties appropriées ne seraient pas garanties, vous êtes tenu de suspendre ou de mettre fin au transfert des données à caractère personnel.

[3] Voir notamment le considérant 145 de l'arrêt de la Cour et la clause 4, point g), de la décision 2010/87/UE de la Commission, ainsi que la clause 5, point a), de la décision 2001/497/CE de la Commission, et l'annexe II, point c), de la décision 2004/915/CE de la Commission.

Toutefois, si vous avez l'intention de continuer à transférer des données malgré cette conclusion, vous devez en informer l'autorité de contrôle dont vous relevez[4].

7) Qu'en est-il des autres outils de transfert en vertu de l'article 46 du RGPD?

➔ Le comité européen de la protection des données évaluera les conséquences de l'arrêt sur les outils de transfert autres que les clauses contractuelles types et les BCR. L'arrêt précise que la norme appliquée en matière de garanties appropriées conformément à l'article 46 du RGPD est celle de «l'équivalence substantielle».

Comme l'a souligné la Cour, il convient de noter que l'article 46 qui figure au chapitre V du RGPD doit, par conséquent, être lu à la lumière de l'article 44 du RGPD, qui prévoit que «*toutes les dispositions du présent chapitre sont appliquées de manière à ce que le niveau de protection des personnes physiques garanti par le présent règlement ne soit pas compromis*».

8) Puis-je avoir recours à l'une des dérogations de l'article 49 du RGPD pour transférer des données vers les États-Unis?

➔ Il est encore possible de transférer des données depuis l'EEE vers les États-Unis sur la base des dérogations prévues à l'article 49 du RGPD, pour autant que les conditions énoncées dans le présent article s'appliquent. Le comité européen de la protection des données renvoie à ses lignes directrices sur cette disposition[5].

Il convient notamment de rappeler que, lorsque les transferts sont fondés sur le consentement de la personne concernée, ledit consentement doit être:

- explicite,
- spécifiquement donné pour le transfert ou l'ensemble de transferts de données en question (ce qui signifie que l'exportateur de données doit s'assurer d'obtenir un consentement spécifique avant la mise en place du transfert, même si cela se produit après la collecte des données), et
- éclairé, en particulier en ce qui concerne les éventuels risques du transfert (autrement dit, la personne concernée doit également être informée des risques spécifiques résultant du fait que ses données seront transférées vers un pays qui ne fournit pas une protection adéquate et qu'aucune garantie appropriée visant à protéger les données n'est mise en œuvre).

En ce qui concerne les transferts nécessaires à l'exécution d'un contrat entre la personne concernée et le responsable du traitement, il convient de garder à l'esprit que les données à caractère personnel peuvent être transférées à condition que le transfert soit occasionnel. Il conviendra de déterminer au cas par cas si les transferts de données seront «occasionnels» ou

[4] Voir notamment le considérant 145 de l'arrêt de la Cour, et la clause 4, point g), de la décision 2010/87/UE de la Commission. Voir également la section 6.3, du document WP256 rev.01 (groupe de travail «Article 29», document de travail établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes, approuvé par le comité européen de la protection des données, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109), et la section 6.3, du document WP257 rev.01 (groupe de travail «Article 29», document de travail établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes pour les sous-traitants, approuvé par le comité européen de la protection des données, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110).

[5] Voir les lignes directrices 2/2018 du comité européen de la protection des données relatives aux dérogations prévues à l'article 49 du règlement (UE) 2016/679, adoptées le 25 mai 2018, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_fr.pdf, p. 3.

«non occasionnels». En tout état de cause, cette dérogation ne peut être invoquée que lorsque le transfert est objectivement nécessaire à l'exécution du contrat.

En ce qui concerne les transferts nécessaires pour des motifs importants d'intérêt public (qui doivent être reconnus par le droit de l'UE ou des États membres[6]), le comité européen de la protection des données rappelle que l'exigence essentielle pour l'applicabilité de cette dérogation consiste à constater un intérêt public important et ne réside pas dans la nature de l'organisation, et bien que cette dérogation ne se limite pas aux transferts de données «occasionnels», cela ne signifie pas que les transferts de données effectués sur la base de la dérogation d'intérêt public important peuvent être réalisés à grande échelle et de manière systématique. Au contraire, il convient de respecter le principe général selon lequel les dérogations prévues à l'article 49 du RGPD ne doivent pas devenir «la règle» en pratique, mais qu'elles doivent se limiter à des situations spécifiques, et que chaque exportateur de données doit s'assurer que le transfert répond au critère de stricte nécessité.

9) Puis-je continuer à utiliser des clauses contractuelles types ou des BCR pour transférer des données vers un pays tiers autre que les États-Unis?

➔ La Cour a indiqué que les clauses contractuelles types peuvent toujours, en règle générale, être utilisées pour transférer des données vers un pays tiers, mais le seuil fixé par la Cour pour les transferts effectués vers les États-Unis s'applique à tout pays tiers. Il en va de même pour les BCR.

La Cour a souligné qu'il incombe à l'exportateur de données et à l'importateur de données d'évaluer si le niveau de protection requis par le droit de l'UE est respecté dans le pays tiers concerné afin de déterminer si les garanties établies par les clauses contractuelles types ou par les BCR le peuvent être respectées dans la pratique. Si tel n'est pas le cas, vous devez vérifier que vous pouvez prévoir des mesures supplémentaires permettant d'assurer un niveau de protection substantiellement équivalent à celui établi dans l'EEE, et que la législation du pays tiers n'affecte pas ces mesures supplémentaires au point d'en compromettre l'efficacité.

Vous pouvez contacter votre importateur de données pour vérifier la législation en vigueur dans son pays et collaborer en vue de son évaluation. Si vous déterminez, ou si l'importateur de données du pays tiers détermine, que les données transférées en vertu des clauses contractuelles types ou des BCR ne bénéficient pas d'un niveau de protection substantiellement équivalent à celui garanti dans l'EEE, vous devez immédiatement suspendre les transferts. Dans le cas contraire, vous devez en informer l'autorité de contrôle dont vous relevez[7].

➔ Comme l'a souligné la Cour, bien qu'il relève de la responsabilité principale des exportateurs et des importateurs de données de vérifier si la législation en vigueur dans le pays tiers de destination permet à l'importateur de données de se conformer aux clauses types de protection des données ou aux BCR, avant de transférer des données à caractère personnel vers ce pays tiers, les autorités de contrôle compétentes auront également un rôle clé à jouer lors de l'application du RGPD et lors de la prise de décisions supplémentaires relatives aux transferts vers des pays tiers.

[6] On entend par «États membres» les États membres de l'Espace économique européen.

[7] Voir notamment le considérant 145 de l'arrêt de la Cour. En ce qui concerne les clauses contractuelles types, voir la clause 4, point g), de la décision 2010/87/UE de la Commission, ainsi que la clause 5, point a), de la décision 2001/497/CE de la Commission, et l'annexe II, point c), de la décision 2004/915/CE de la Commission. En ce qui concerne les BCR, voir la section 6.3, du document WP256 rev.01 (approuvé par le comité européen de la protection des données) et la section 6.3, du document WP257 rev.01 (approuvé par le comité européen de la protection des données).

Comme l'a suggéré la Cour, afin d'éviter de prendre des décisions divergentes, ils travailleront, par conséquent, davantage au sein du comité européen de la protection des données afin d'assurer la cohérence, en particulier si des transferts vers des pays tiers doivent être interdits.

10) Quel type de mesures supplémentaires puis-je introduire si j'utilise des clauses types de protection des données ou des BCR pour transférer des données vers des pays tiers?

➔ Les mesures supplémentaires que vous pourriez envisager, le cas échéant, devront être fournies au cas par cas, en fonction de toutes les circonstances du transfert et après l'évaluation de la législation en vigueur dans le pays tiers, laquelle permettra de vérifier si cette législation garantit un niveau de protection adéquat.

La Cour a souligné qu'il incombe exclusivement à l'exportateur de données et à l'importateur de données de procéder à cette évaluation et de fournir les mesures supplémentaires nécessaires.

Le comité européen de la protection des données analyse actuellement l'arrêt de la Cour afin de déterminer le type de mesures supplémentaires qui pourraient être fournies en plus des clauses types de protection des données ou des BCR, qu'il s'agisse de mesures juridiques, techniques ou organisationnelles relatives au transfert de données vers des pays tiers, dans le cas où les clauses types de protection des données ou les BCR n'assureraient pas un niveau suffisant de garanties.

➔ Le comité européen de la protection des données examine actuellement de manière approfondie en quoi ces mesures supplémentaires pourraient consister et fournira davantage de lignes directrices à cet égard.

11) J'utilise les services d'un sous-traitant qui traite les données dont je suis responsable en tant que responsable des données. Comment puis-je savoir si ce sous-traitant transfère des données vers les États-Unis ou vers un autre pays tiers?

➔ Le contrat que vous avez conclu avec votre sous-traitant conformément à l'article 28, paragraphe 3, du RGPD, doit indiquer si les transferts sont autorisés ou non (il convient de rappeler que même le fait d'autoriser un pays tiers à accéder aux données, par exemple à des fins administratives, équivaut également à un transfert).

➔ Il convient également d'autoriser les sous-traitants à confier aux sous-traitants ultérieurs le transfert de données vers des pays tiers. Soyez attentif et prudent, car une grande variété de solutions informatiques peut impliquer le transfert de données à caractère personnel vers un pays tiers (par exemple, à des fins de stockage ou de maintenance).

12) Que puis-je faire pour continuer à utiliser les services de mon sous-traitant si le contrat signé conformément à l'article 28, paragraphe 3, du RGPD, indique que les données peuvent être transférées vers les États-Unis ou vers un autre pays tiers ?

➔ Si vos données peuvent être transférées vers les États-Unis et qu'aucune mesure supplémentaire ne peut être fournie pour s'assurer que le droit des États-Unis n'affecte pas le niveau de protection substantiellement équivalent, tel qu'il est garanti dans l'EEE par les outils de transfert, les dérogations prévues à l'article 49 du RGPD ne s'appliquent pas non plus; la seule solution consiste à négocier une modification ou une clause supplémentaire à votre contrat pour interdire les transferts vers les États-Unis. Les données doivent être stockées, mais également administrées ailleurs qu'aux États-Unis.

➔ Si vos données peuvent être transférées vers un autre pays tiers, vous devez également vérifier que la législation en vigueur dans ce pays tiers est conforme aux exigences de la Cour et au niveau de protection des données à caractère personnel escompté. Si aucun arrangement convenable

n'est trouvé en matière de transfert vers un pays tiers, les données à caractère personnel ne doivent pas être transférées en dehors du territoire de l'EEE et toutes les activités de traitement doivent être réalisées dans l'EEE.

Pour le comité européen de la protection des données

La présidente

Andrea Jelinek