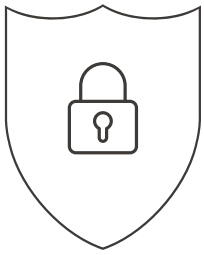
RENAISSANCE numérique

LIBERTÉS PUBLIQUES ET ÉTHIQUE
JANVIER 2021

ARRÊT SCHREMS II :

Comment sortir de l'impasse ?



Le 16 juillet 2020, dans son arrêt dit « Schrems II », la Cour de justice de l'Union européenne (CJUE) a invalidé l'accord encadrant les transferts transatlantiques de données — *Privacy Shield* ou Bouclier de protection des données UE-États-Unis. Dans le cadre de cette décision, la Cour a estimé que cet accord n'apportait pas les garanties suffisantes pour la protection des données personnelles des citoyens européens[1].

Si cette décision historique a fait l'objet de quelque peu d'attention médiatique lors de sa parution, cet intérêt public est depuis retombé. Or, cet arrêt a plongé nombre d'acteurs dans une période d'incertitude et d'insécurité juridique, qui s'installe désormais dans la durée. Au premier rang des acteurs concernés, les entreprises européennes : selon une enquête conduite par plusieurs fédérations d'entreprises de l'Union européenne auprès de leurs membres, 75 % des entreprises qui utilisent les clauses contractuelles types pour les transferts internationaux de données sont européennes, et ce, quelle que soit leur taille[2]. Les citoyens européens ne sont, eux-mêmes, pas épargnés par les conséquences de cette décision, puisqu'ils bénéficiaient jusqu'alors, avec le *Privacy Shield*, d'un système de protection de leurs données. Si celui-ci était imparfait, il se retrouve désormais mis en arrêt et non remplacé.

Dans ce contexte, Renaissance Numérique a organisé, le 16 décembre dernier, un séminaire réunissant une trentaine de représentants d'entreprises, juristes, universitaires, parlementaires et représentants de l'administration. L'objectif de cette discussion était double : explorer les conséquences de la décision de la Cour de Justice de l'Union européenne, et envisager des pistes de résolution pour les acteurs concernés par cette dernière. Cette note est

1 « La Cour invalide la décision 2016/1250 relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis », Cour de justice de l'Union européenne, communiqué de presse n° 91/20, 16 juillet 2020 : https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091fr.pdf

2 Parmi les entreprises répondantes. « Schrems II. Impact Survey Report », DIGITALEUROPE, BusinessEurope, the European Round Table for Industry (ERT) and ACEA, 26 novembre 2020 : https://www.businesseurope.eu/publications/schrems-ii-impact-survey-report

nourrie de ces échanges[3].

De cette discussion, ressortent beaucoup d'inquiétudes quant à la capacité des acteurs à mettre en œuvre l' « arrêt Schrems II ». Non seulement il n'offre pas pour les acteurs de délai de grâce permettant de l'analyser en profondeur, ainsi que d'évaluer l'applicabilité des recommandations portées par les autorités de protection des données à sa suite, mais il est également rétroactif. Ainsi, au-delà des transferts internationaux de données à venir, la conformité de tous les transferts opérés sous le *Privacy Shield* depuis 2016 doit être réévaluée, remettant en question une multitude de contrats actuels. Des premières plaintes ont déjà été déposées dans la lignée de cet arrêt, dont plusieurs à l'encontre d'entreprises françaises[4]. Or, la conclusion de ces procédures, et donc la jurisprudence afférente, ne devraient pas intervenir avant l'été 2021. D'ici là, si aucune décision politique n'est prise, de nombreuses activités seront menacées, à l'heure où les données jouent un rôle essentiel pour notre économie.

Au-delà d'un débat juridique, la décision de la Cour de Justice de l'Union européenne revêt ainsi de fortes dimensions économique et politique qui ne peuvent être laissées aux seules mains des régulateurs. Dans un contexte incertain, où des inconnues demeurent encore sur ce que sera la position de l'administration du nouveau président américain en la matière, cette situation pose la question de l'efficience du modèle de protection européen.

Face à cette impasse, Renaissance Numérique invite, au travers de cette réflexion, la Commission européenne et l'exécutif européen à ouvrir un dialogue avec les parties prenantes, afin d'établir une méthode partagée pour la mise en œuvre de cette décision.

De Schrems I à Schrems II

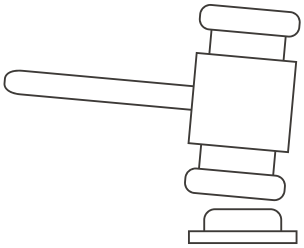
Le caractère hautement technique de ce débat semble participer du désintérêt politique, malgré des conséquences particulièrement tangibles pour les acteurs concernés. Aussi, il convient de bien appréhender les contours de cette décision.

---

3 Renaissance Numérique remercie l'ensemble des participants au séminaire du 16 décembre 2020 qui ont nourri cette réflexion, et en particulier Florence Raynal, Cheffe du service des affaires européennes et internationales de la CNIL, Théodore Christakis, Professeur de droit international et européen à l'Université Grenoble Alpes, Juliette Rouilloux-Sicre, Présidente du Comité Régulations du numérique du MEDEF et Etienne Drouard, Partner chez Hogan Lovells, qui ont permis d'introduire ce débat.

4 L'association noyb (https://noyb.eu/), créée par Max Schrems, a porté plainte contre plusieurs entreprises françaises à l'instar de Leroy Merlin, Sephora et Decathlon. « La fin du *Privacy Shield* : sortons les entreprises de cet imbroglio juridique ! » Jean-Sébastien Mariez, *JDN*, 21 décembre 2020 : https://www.journaldunet.com/solutions/dsi/1496487-la-fin-du-privacy-shield-sortons-les-entreprises-de-cet-imbroglio-juridique

Elle s'inscrit dans le cadre du Règlement général sur la protection des données (RGPD), entré en application en mai 2018 et qui institue le principe selon lequel la protection accompagne la donnée, où qu'elle soit transférée dans le monde. Dès lors, la donnée peut être transférée uniquement si la protection dans le pays destinataire est essentiellement équivalente à celle offerte au sein de l'Union européenne (UE), sauf dérogations particulières[5]. Plusieurs outils peuvent apporter ce degré équivalent de protection, tels que les décisions d'adéquation de la Commission européenne comme le *Privacy Shield*, qui reconnaissent que le régime juridique du pays destinataire respecte le droit de l'Union européenne. Cette protection peut également être assurée de manière contractuelle, à l'instar des BCR (*Binding Corporate Rules*) et des clauses contractuelles types ou *ad hoc*, ou au travers de la certification et des codes de conduite. Un certain nombre de ces outils de transfert sont en train d'être adaptés à la suite de l'arrêt du 16 juillet 2020. Mais, jusqu'à présent, ils n'apportent pas plus de précisions sur les mesures à mettre en œuvre, et donc de solutions pour les acteurs, que la décision elle-même.



Le premier arrêt de la CJUE en ce domaine, rendu fin 2015, dit « Schrems I », reposait sur un différend entre le militant autrichien Max Schrems et Facebook[6]. Max Schrems considérait que le *Safe Harbor* — prédécesseur du *Privacy Shield* — n'apportait pas une protection suffisante aux données personnelles des citoyens européens qui étaient transférées par Facebook vers les États-Unis. Lors de ce premier jugement, la Cour a jugé que les États-Unis n'assuraient pas des protections essentiellement équivalentes à celles portées par le droit européen. Elle a invalidé le *Safe Harbor* et invité la Commission européenne à revoir sa copie.

Le deuxième recours de Max Schrems, qui a donné lieu à l'arrêt « Schrems II », a porté, cette fois-ci, sur les clauses contractuelles types utilisées par Facebook pour réaliser ses transferts[7]. En effet, le *Safe Harbor* n'existant plus, Facebook s'est reporté sur les clauses contractuelles types. La question était alors de savoir si ces clauses apportaient une protection suffisante[8]. La Cour de justice de l'Union européenne a considéré que les clauses contractuelles types en tant que telles sont valides, parce qu'elles ne restent qu'un outil qui comprend des obligations contractuelles, et que les garanties contenues dans ces clauses ne posent pas de difficultés. Ce qui pose un problème c'est

5 « CHAPITRE V — Transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales », Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données). Détails sur le site de la CNIL: https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre5#Article44

6 Arrêt « C-362/14 — Schrems », Cour de justice de l'Union européenne, 6 octobre 2015 : http://curia.europa.eu/juris/liste.jsf?language=fr&num=C-362/14

7 Arrêt « C-311/18 — Facebook Ireland et Schrems », Cour de justice de l'Union européenne, 16 juillet 2020: http://curia.europa.eu/juris/liste.jsf?language=fr&num=C-311/18

8 « Demande de décision préjudicielle présentée par la High Court (Irlande) le 9 mai 2018 — Data Protection Commissioner / Facebook Ireland Limited, Maximilian Schrems », Cour de justice de l'Union européenne : http://curia.europa.eu/juris/document/document.jsf?text=&docid=204046&pageIndex=0&doclang=FR&mode=req&dir=&occ=first&part=1&cid=23307047

le lien entre les garanties contractuelles et le droit du pays destinataire qui recevra ces données. L'enjeu est de savoir si le droit de ce pays permettra à l'importateur de respecter ses obligations contractuelles. Le problème soulevé par cet arrêt est le conflit possible avec le droit du destinataire, notamment avec les lois américaines de renseignement[9], qui, en l'espèce, ne permettent pas à l'importateur de respecter ses engagements. Auparavant, la logique juridique encadrant ces transferts était de s'assurer que l'importateur respecte les garanties prévues dans le contrat. Désormais, la logique est plus large, puisqu'il faut aussi s'assurer qu'il n'y a pas de conflits avec d'autres instruments juridiques ou normes ayant une valeur juridique supérieure. Le raisonnement s'applique à tous les pays et à tous les outils de protection : si la loi du pays ne permet pas de respecter les garanties essentielles[10], la protection, quel que soit l'instrument, n'existe pas.

Une interprétation stricte par les régulateurs qui pèse lourdement sur les acteurs

À la suite de cette décision, le 10 novembre 2020, l'*European Data Protection Board* (EDPB), qui réunit les autorités nationales de protection des données, a publié une mise à jour des « Garanties essentielles européennes pour les mesures de surveillance »[11]. Ces dernières avaient été élaborées en 2016, au moment de la négociation du *Privacy Shield*. Elles constituent une sorte de guide, qui pose notamment les conditions à respecter lorsqu'il y a une interférence par un gouvernement avec les droits fondamentaux. En parallèle de ce texte, le comité européen a produit un autre document qui porte des recommandations sur des mesures visant à compléter les outils de transferts internationaux, pour garantir le respect du niveau de protection des données personnelles de l'UE[12] [13]. Il offre une méthodologie aux organisations qui transfèrent et reçoivent des données, dans le cas où le régime juridique en question ne présenterait pas les garanties suffisantes. Ces mesures peuvent être de l'ordre contractuel, organisationnel ou technique, ces dernières étant privilégiées par l'EDPB.

---

9 Le juge s'est notamment prononcé sur le *Foreign Intelligence Surveillance Act* (FISA) et l'*Executive Order 12333*, qui font partie du régime juridique américain en matière de surveillance.

10 Cf. infra.

11 « Recommendations 02/2020 on the European Essential Guarantees for surveillance measures », *European Data Protection Board*, 10 novembre 2020 : https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf

12 « Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data », *European Data Protection Board*, 10 novembre 2020 : https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

13 Il était en consultation publique jusqu'au 21 décembre 2020.

Or, cet arrêt fait peser une responsabilité extrêmement importante sur les organisations qui transfèrent des données à l'international et les recommandations induites par l'EDPB peuvent apparaître difficilement applicables. D'une part, les mesures techniques, à l'instar du chiffrement, revêtent un coût significatif, qui pourrait empêcher la rentabilité de nombre d'activités[14]. D'autre part, concernant les garanties essentielles, l'EDPB retient des critères extrêmement stricts. Les entreprises, qu'elles soient des TPE ou des grands groupes, n'ont pas les moyens d'analyser les lois de surveillance de l'ensemble des pays tiers. Une analyse juridique des lois de surveillance peut, par exemple, s'élever à 250 000 dollars pour le seul régime américain. Il conviendrait également que cette analyse soit partagée entre les acteurs, afin d'éviter toute erreur d'interprétation qui pourrait leur coûter cher.

Enfin, et c'est peut-être la limite principale de l'interprétation de l'*European Data Protection Board*, très peu de pays atteignent le niveau de ces garanties essentielles, y compris les États membres de l'Union européenne, dont la France. Si on analyse toutes les lois de surveillance des pays du Conseil de l'Europe qui ont été portées depuis 2001 devant la Cour européenne des droits de l'homme (CEDH), aucun pays ne passe le test, hormis un, la Suède[15]. Cet arrêt est toutefois contesté par les requérants et demeure pendant devant la Grande Chambre de la Cour[16]. De même, dans ses arrêts du 6 octobre 2020 sur la conservation et la transmission des données[17], la Cour de justice de l'Union européenne a jugé qu'un certain nombre de pratiques des États membres, dont la France, en matière de renseignement, ne répondaient pas aux normes européennes.

Actuellement, il y a au moins quatorze requêtes en traitement contre les lois de surveillance en France[18]. En vingt ans, la Commission européenne n'a été capable d'accorder une décision d'adéquation qu'à seulement onze pays[19]. Parmi ces derniers, pour lesquels les décisions d'adéquation sont désormais en réévaluation, on peut également s'interroger si tous respectent les garanties essentielles, à l'instar d'Israël.

Lors de l'examen du projet de loi « Renseignement » ayant abouti à la création de la CNCTR[20], Renaissance Numérique avait relevé, en mai 2015, que

14 Au-delà du coût, selon leur finalité, le risque du chiffrement ou de la pseudonymisation est également que les données deviennent inexploitables par le destinataire.

15 « Affaire Centrum för Rättvisa c. Suède », Cour européenne des droits de l'homme : https://hudoc.echr.coe.int/eng#%7B%22languageisocode%22:%5B%22FRE%22%5D,%22appno%22:%5B%2235252/08%22%5D,%22documentcollectionid2%22:%5B%22CHAMBER%22%5D,%22itemid%22:%5B%22001-184290%22%5D%7D

16 Théodore Christakis, « "Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 1) », *European Law Blog*, novembre 2020 : https://europeanlawblog.eu/2020/11/13/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-1/

17 Privacy international (aff. C-623/17) : https://cdn2.nextinpact.com/medias/arret-c_623_17fr.pdf, et La Quadrature du Net, French Data Network et autres : https://cdn2.nextinpact.com/medias/arret-c_511_18fr.pdf (aff. jointes C-511/18, C-512/18, C-520-18), Cour de justice de l'Union européenne, 6 octobre 2020.

18 « Surveillance de masse », Fiche thématique, Cour européenne des droits de l'homme, octobre 2020.

19 « Adequacy decisions », Commission européenne : https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

20 Commission nationale de contrôle des techniques de renseignement.

le cadre juridique envisagé[21] ne prévoyait pas de contrôle indépendant ou à caractère juridictionnel, ni même de recours effectif pour les personnes concernées. À cet égard, les critères procéduraux dégagés par la Cour européenne des droits de l'homme pour satisfaire les exigences de finalité et de proportionnalité et qui ont été repris par la CJUE dans l'arrêt Schrems II, ne semblaient pas satisfaits par le cadre juridique en vigueur[22].

Les institutions européennes, qui disposent d'un haut niveau d'expertise juridique, auquel les entreprises n'ont pas accès, ont elles-mêmes émis un jugement erroné à quatre reprises : avec le *Safe Harbor*, le *Privacy Shield*, avec les *Passenger Name Records* (PNR) avec les États-Unis[23] et le Canada[24]. Comment les entreprises pourraient-elles être mieux outillées pour répondre à ces exigences ? Le risque est double : soit qu'elles se ruinent à coups de frais juridiques, soit qu'elles entrent dans une logique de non-conformité, qui serait extrêmement préjudiciable pour le RGPD et les citoyens européens.

Une décision qui dépasse le seul champ du droit des données personnelles

Au-delà de leur caractère strict, ces recommandations semblent, par ailleurs, omettre le principe essentiel de la hiérarchie des normes, qui est à la base du droit. Derrière cette décision, apparaît en effet un conflit de souveraineté entre États, puisque cet arrêt considère que les lois d'un pays ne sont pas suffisantes pour justifier le transfert de données vers ce dernier. L'enjeu se trouve sur l'accès des gouvernements à des données qui sont protégées par d'autres droits. Or, aucun acteur ne peut promettre officiellement qu'il dérogera aux lois souveraines qui s'imposent à lui. Considérant la hiérarchie des normes, il est compliqué que des clauses contractuelles types puissent répondre à un conflit de souveraineté, donc à des lois qui sont des normes supérieures. Ainsi, au-delà du champ de la protection des données

21 Consacré par la loi 2015-912 du 24 juillet 2015.

22 En particulier, les pouvoirs conférés à la CNCTR la confinent à exercer un contrôle documentaire préalable de la régularité formelle des mesures de contrôle. Toutefois, la CNCTR ne dispose pas de pouvoirs effectifs de contrôle de la pertinence ou de la proportionnalité des mesures de surveillance envisagées (contrôle *a priori*) ou mises en œuvre (contrôle *a posteriori*). En outre, les voies de recours accessibles sous la condition d'un intérêt personnel à agir sont vidées de leur substance par la confidentialité des mesures de surveillance qui, par nature, ne permettent pas à une personne de savoir si — ou de démontrer que — elle fait l'objet de mesures de surveillance.

23 « The Court annuls the Council decision concerning the conclusion of an agreement between the European Community and the United States of America on the processing and transfer of personal data and the Commission decision on the adequate protection of those data », Cour de justice des communautés européennes, 30 mai 2006 : https://curia.europa.eu/en/actu/communiques/cp06/aff/cp060046en.pdf

24 « La Cour déclare que l'accord sur le transfert des données des dossiers passagers, prévu entre l'Union européenne et le Canada, ne peut pas être conclu sous sa forme actuelle », Cour de justice de l'Union européenne, 26 juillet 2017 : https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-07/cp170084fr.pdf

personnelles, l'analyse de l'application de cet arrêt nécessite de s'intéresser à d'autres disciplines du droit, que sont notamment le droit international et le droit constitutionnel.

À ce titre, cette décision soulève également le conflit naturel en matière de droits fondamentaux, entre les lois de surveillance et de protection de la vie privée. Ce dernier existe depuis toujours. Ces droits sont combinatoires. Quelle entreprise va pouvoir se soustraire à une loi nationale, si jamais on lui demande de fournir des données pour des raisons de sécurité ? L'Union européenne invoque le RGPD, là où d'autres États mettent en jeu leur économie et leur sécurité nationales. La balance entre la sécurité et la liberté ne s'arbitre pas dans le RGPD, qui est un texte sur les libertés. Dès lors, l'interprétation de cette décision dépasse du champ d'expertise des autorités de protection des données, qui ne sont ni des constitutionnalistes, ni des spécialistes de l'antiterrorisme. La question qui se pose ici est celle de l'équilibre entre droits fondamentaux, de la conformité à la Convention européenne des droits de l'homme. À ce titre, la décision de la Cour de justice de l'Union européenne offre une marge de manœuvre pour garantir cet équilibre et son applicabilité.

Cet équilibre pose d'autant plus de questions à l'heure où les initiatives législatives visant à organiser l'accès des autorités publiques aux données chiffrées se multiplient à travers l'Union européenne. Cette tendance est illustrée par la résolution sur le chiffrement, adoptée par le Conseil de l'Union européenne le 14 décembre dernier, dont l'objet est notamment de permettre l'accès des pouvoirs d'enquête et judiciaires à ces données[25].

Un agenda désormais incertain

Ces problématiques relèvent du régalien et, dès lors, devraient être portées par la Commission européenne et l'exécutif européen, ainsi que par les États membres. Alors que régulateurs et entreprises se renvoient la responsabilité, la situation perdure au risque de fragiliser pour longtemps nombre d'acteurs. La question n'est plus comment sortir de l'impasse, mais qui va sortir l'Union européenne de cette impasse. Il semblerait aujourd'hui que ce sujet passe en arrière-plan des grands dossiers numériques qui sont traités par la Commission européenne, à l'instar du *Digital Services Act* et du *Digital Mar-*

25 « Chiffrement : adoption par le Conseil d'une résolution intitulée "La sécurité grâce au chiffrement et malgré le chiffrement" », Conseil de l'Union européenne, 14 décembre 2020 : https://www.consilium.europa.eu/fr/press/press-releases/2020/12/14/encryption-council-adopts-resolution-on-security-through-encryption-and-security-despite-encryption/?utm_source=dsms-auto&utm_medium=email&utm_campaign=Encryption:+Council+adopts+resolution+on+security+through+encryption+and+security+despite+encryption

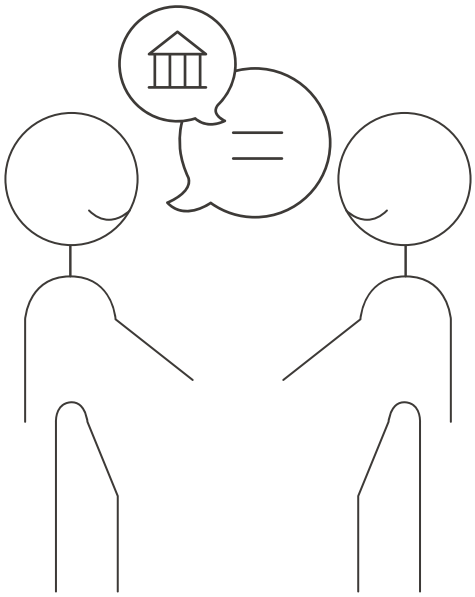
kets Act parus en décembre. Or, il est plus que temps de s'en saisir.

Alors que l'arrêt Schrems II ne fait pas l'objet d'une période de grâce, Renaissance Numérique appelle la Commission européenne et l'exécutif européen à ouvrir une concertation avec les parties prenantes, afin que l'interprétation qui est faite de la décision de la Cour de justice de l'Union européenne donne lieu à une mise en œuvre harmonisée au sein de l'Union européenne. Ce dialogue devrait permettre aux instances européennes de réunir les expertises pertinentes, au-delà du seul champ de la protection des données — spécialistes du droit constitutionnel, du droit international et des questions de surveillance notamment. Cela leur permettrait ainsi de définir une grille de lecture établissant les critères à respecter, et, sur cette base, d'identifier les solutions adéquates déjà en place et d'envisager des pistes de résolution.

À ce titre, cela permettrait également d'évaluer l'applicabilité des solutions proposées par l'EDPB et de les traduire, le cas échéant, en critères plus lisibles pour les entreprises ou en solutions tangibles.

Dans ce cadre, Renaissance Numérique invite à développer une approche proportionnée des risques, tenant compte en particulier de la sensibilité des données transférées. Concernant les données hautement sensibles, des mesures renforcées pourraient être envisagées, à la différence d'autres données moins sensibles. Cette étape intermédiaire permettrait de ne pas rester dans l'impasse en attendant la conclusion d'un nouvel accord international robuste.

À l'heure où les États sont en conflit de souveraineté dans le champ numérique, la résolution, à terme, ne pourra, en effet, passer que par la signature d'un nouvel accord avec les États-Unis.



Pour aller plus loin

« La Cour invalide la décision 2016/1250 relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis », Cour de justice de l'Union européenne, communiqué de presse n° 91/20, 16 juillet 2020 : https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091fr.pdf

« Recommendations 02/2020 on the European Essential Guarantees for surveillance measures », *European Data Protection Board*, 10 novembre 2020 : https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf

« Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data », *European Data Protection Board*, 10 novembre 2020 : https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

Théodore Christakis, « "Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers (Part 1 , Part 2 & Part 3) », *European Law Blog*, novembre 2020 : Part 1 : https://europeanlawblog.eu/2020/11/13/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-1/ Part 2 : https://europeanlawblog.eu/2020/11/16/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-2/ Part 3 : https://europeanlawblog.eu/2020/11/17/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-3/

—

Rédaction

Jennyfer Chrétien, Déléguée générale, Renaissance Numérique

Contribution

Loane Bedouet, Chargée de mission, Renaissance Numérique

Etienne Drouard, Associé chez Hogan Lovells

Relecture

Jessica Galissaire, Responsable des études, Renaissance Numérique

Nous remercions également **Théodore Christakis**, Professeur de droit international et européen à l'Université Grenoble Alpes, pour le partage de son expertise.