DOCTRINE

DONNÉES PERSONNELLES

Quatre mois après Schrems 2, l'impasse demeure

Ni les recommandations du CEDP ni le projet de nouvelles clauses contractuelles de la Commission européenne n'apportent de solution satisfaisante pour transférer en toute sécurité juridique des données personnelles hors de l'Union européenne.

L'arrêt Schrems 2[1] rendu par la Cour de justice de l'Union européenne le 16 juillet dernier était attendu et n'a pas constitué une véritable surprise. En interdisant les transferts vers les Etats-Unis sur la base du Privacy Shield et en rendant quasi inopérantes les clauses contractuelles types proposées par la Commission européenne, il pose cependant des problèmes pratiques qui ne semblent pas pouvoir être surmontés, malgré les efforts récents du Comité européen de la protection des données (CEPD) et de la Commission européenne. Ces deux institutions communautaires ont chacune, respectivement le 10 et le 12 novembre, essayé d'apporter des réponses à ces problèmes. Le CEPD a publié des recommandations sur les mesures qui complètent les outils de transfert pour assurer le respect des niveaux de protection des données personnelles de l'UE et la Commission a annoncé un nouveau projet de clauses contractuelles types.

L'arrêt Schrems 2

Suite au renvoi de son dossier devant l'autorité de contrôle irlandaise après la décision de la Cour de justice de l'Union européenne du 6 octobre 2014[2] annulant le mécanisme de Safe Harbour, Maximilien Schrems a reformulé sa plainte devant le Data Protection Commissioner (l'autorité de contrôle irlandaise) et a demandé, au vu de l'obligation faite à Facebook Ireland Ltd (Facebook) de transférer ses données aux autorités américaines telles que la NSA ou le FBI selon la législation américaine, d'interdire le transfert de ses données par Facebook. Ce transfert était en effet désormais justifié par Facebook par la conclusion d'un contrat de transfert de données sur la base des Clauses contractuelles types (« *CCT* ») émises par la Commission européenne dans sa décision 2010/87. M. Schrems, dans sa plainte, a estimé qu'au vu de la réglementation américaine, ces CCT ne pouvaient assurer un niveau de protection de ses données personnelles conforme à la Charte des droits fondamentaux[3] (la Charte). Le Data Protection Commissioner a accueilli les arguments de M. Schrems mais, estimant que ces arguments remettaient en cause la validité de la décision de la Commission européenne autorisant les CCT de responsable à sous-traitant[4], a saisi la High Court irlandaise pour qu'elle puisse interroger la CJUE sur cette question, ce qu'elle a fait par un arrêt du 3 octobre 2017[5] dans lequel elle a procédé à une description très détaillée de la réglementation américaine permettant la surveillance des données personnelles de ressortissants étrangers, et en particulier des programmes PRISM et UPSTREAM. La saisine de la Cour portait essentiellement sur la validité des CCT mais concernant également la validité du Privacy Shield[6] (le mécanisme renforcé négocié par la Commission afin de remplacer le Safe Harbour) puisqu'elle demandait si la décision adoptant le Privacy Shield « *constituait une constatation d'application générale liant les autorités en charge de la protection des données et les juridictions des Etats membres selon laquelle les Etats-Unis assurent un niveau de protection adéquat au sens de l'article 25.2 de la directive 95/46 en raison de leur droit interne ou de leurs engagements internationaux* ».

Sur la légalité du Privacy Shield

Tout comme dans l'arrêt Schrems 1, la Cour a élargi sa saisine sur cette question. Elle a tout d'abord jugé que la décision de la Commission adoptant le Safe Harbour, qui constatait que « *les Etats-Unis assurent un niveau adéquat de protection de données à caractère personnel transférées depuis l'Union vers des organisation établies aux Etats-Unis dans le cadre du bouclier de protection des données* » avait un caractère contraignant pour les autorités de contrôles. Ces dernières doivent néanmoins, si elles ont un doute sur sa validité saisir les juridictions nationales pour qu'elles puissent faire parvenir une question préjudicielle à la CJUE à ce sujet. Ceci est une répétition de son raisonnement dans l'arrêt Schrems 1. La Cour a ensuite jugé qu'afin de donner une réponse complète à la question posée, elle devait examiner si la décision Safe Harbour était conforme aux exigences du RGPD, lu à la lumière de la Charte. La réponse à cette question n'a généré que peu d'étonnement au vu de la jurisprudence antérieure de la Cour.

La Commission avait, dans sa décision adoptant le Privacy Shield, procédé à une analyse très détaillée de la législation américaine concernant l'accès aux données de ressortissants étrangers pour des raisons de sécurité nationale, et estimé que « *sur la base des informations disponibles concernant l'ordre juridique des Etats-Unis, ... toute ingérence des autorités publiques américaines dans l'exercice des droits fondamentaux des personnes dont les données sont transférées de l'Union Européenne vers les Etats-Unis dans le cadre du bouclier de protection des données pour les besoins de la sécurité nationale, de l'intérêt public ou du respect des lois, et partant, les restrictions imposées aux organisations autocertifiées en ce qui concerne leur respect des principes seront limités à ce qui est strictement nécessaire pour atteindre l'objectif légitime visé et qu'il existe une protection juridictionnelle effective contre des ingérence de cette nature.* »

Le débat ne porte en effet pas sur le droit des États étrangers à traiter à des fins de sécurité nationale les données personnelles des ressortissants européens qui leur sont transférées mais sur la proportionnalité de ces traitements et sur l'existence de recours juridiques des personnes concernées. La Cour rappelle que si la communication et la conservation de données personnelles aux autorités publiques constitue une ingérence dans les droits fondamentaux au respect de la vie privée consacrés aux articles 7 et 8 de la Charte, elles sont néanmoins possibles sous réserve que ces ingérences soient nécessaires, proportionnées et répondent effectivement à des motifs d'intérêt général.
En utilisant les observations de la Commission dans la décision Privacy Shield sur la législation américaine en la matière, la Cour a constaté que les programmes mis en œuvre par les autorités américaines étaient des programmes généraux et non individuels, avec un contrôle limité au respect de l'objectif d'obtenir des informations en matière de renseignement extérieur mais ne portant pas sur le fait de savoir si les personnes étaient correctement ciblées pour se procurer des informations en matière de renseignement extérieur. De plus, les personnes ciblées ne disposent d'aucun droit opposable aux autorités américaines devant les tribunaux, ce qui disqualifie quasi-automatiquement le programme de Privacy Shield au vu de l'exigence d'un droit de recours effectif selon les termes de l'article 45.2.a du RGPD, le mécanisme de médiation mis en place par le Privacy Shield ne suffisant pas à pallier cette limitation du droit à une protection juridictionnelle, qui plus est au vu de l'absence d'indépendance du médiateur envers le ministre des Affaires étrangères des Etats-Unis.
La Cour a donc pris la décision attendue par les observateurs d'invalider le Privacy Shield et, en l'absence d'une évolution significative de la réglementation américaine du traitement des données des personnes étrangères, un mécanisme de remplacement semble improbable.

Il convient de noter qu'en l'espace de six mois, la Cour a imposé, sur la base de la Charte, ses standards concernant le traitement des données à caractère personnel pour des raisons de sécurité à la fois aux Etats non membres mais aussi aux Etats membres de l'Union européenne. En effet, la Cour a jugé le 6 octobre dernier[7], sur la base de la directive 2002/57 concernant la protection de la vie privée dans le secteur des communications électroniques interprétée à la lumière de la Charte, que les États membres (en l'espèce la France et la Belgique) ne pouvaient pas procéder à une conservation généralisée et indifférenciée des données relatives au trafic et de données de localisation. Elle a encadré strictement le recours à l'analyse automatisée ainsi qu'au recueil en temps réel de ces données, imposant que ces traitements soient faits dans le cadre de menaces graves pour la sécurité nationale identifiées, fassent l'objet d'un contrôle effectif par une juridiction ou une autorité administrative indépendante et soient limités aux personnes qui font l'objet de soupçon d'activité terroriste pour une raison valable. Malgré les précautions prises par les Etats membres pour limiter l'application de la Charte et s'assurer qu'elle ne soit pas utilisée pour étendre les compétences de l'Union européenne (en particulier dans son article 51 rédigé spécialement à cet effet), on ne peut que constater l'interprétation extensive de la Charte par la Cour, puisqu'elle lui permet désormais de juger les mesures de sécurité nationale prises par les Etats membres.

Par ces deux jurisprudences, la Cour s'attaque à deux questions au cœur des prérogatives régaliennes de l'Etat, la sécurité et les relations internationales, sur lesquelles les compétences européennes sont plus que limitées et font l'objet de vives contestations.
Sur ces questions ultra-sensibles en ces temps de terrorisme, on peut s'interroger si la Cour a la légitimité politique et institutionnelle pour prescrire aux Etats membres (et aux Etats étrangers) avec ce niveau de détail comment organiser la défense de leurs citoyens et si une attitude plus respectueuse du principe de subsidiarité n'aurait pas été préférable. Il semble évident qu'aucun Etat souverain, et encore plus une puissance comme les Etats-Unis n'acceptera de restreindre ses capacités à lutter contre le terrorisme pour se plier aux injonctions d'un tribunal étranger, alors que le respect de ces exigences est déjà très difficile pour les Etats membres. Il n'est pas interdit de penser qu'une approche plus restrictive dans ces deux dossiers, utilisant par exemple l'ancienne théorie française des actes de gouvernement pour refuser de juger l'évaluation d'une législation étrangère effectuée par la Commission et la subsidiarité et le respect des compétences telles qu'elles résultent des traités pour refuser d'évaluer la législation anti-terroriste des Etats membres aurait présenté, en ces temps de Brexit et de lutte contre le terrorisme, une certaine sagesse, à défaut de continuité avec l'élan jurisprudentiel intégrationniste de la Cour.

Sur les clauses contractuelles types

La High Court irlandaise avait offert à la CJUE un raisonnement adroit lui permettant de lui éviter de s'immiscer dans la souveraineté américaine, en demandant si le RGPD et le droit de l'Union s'appliquaient au traitement de données effectué par les autorités étrangères à des fins de sécurité nationale consécutif au transfert de données entre deux acteurs privés, qui est, lui, indéniablement soumis au RGPD, en particulier au vu des dispositions de l'article 4.2 du Traité de l'Union européenne qui disposent que l'Union européenne «*respecte les fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer son intégrité territoriale, de maintenir l'ordre public et de sauvegarder la sécurité nationale* ».

La Cour rejette cette proposition assez violemment en notant que « *la disposition contenue à l'article 4, paragraphe 2, selon laquelle au sein de l'Union, la sécurité nationale reste la seule responsabilité de chaque Etat membre, concerne exclusivement les Etats membres de l'Union* » et s'accorde donc explicitement le droit de juger les mesures de sécurité nationale d'Etats étrangers même lorsqu'elle ne pourrait pas le faire pour les Etats membres. Au vu de ce considérant, il semble difficile de s'indigner de l'application extraterritoriale de leur droit par les Etats-Unis d'application...

La High Court irlandaise avait ensuite interrogé la CJUE sur la question de savoir si le niveau de protection requis par l'article 46.2.c du RGPD devait être évalué au vu des instruments de droit communautaire (Charte, traité UE, traité FUE, directive 95/46, convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales) ou de la législation interne des États et, dans ce cas, si les pratiques en matière de sécurité nationale dans un ou plusieurs Etats membres devaient être prises en compte. Par cette question, la High Court pointait de manière évidente le paradoxe d'une Union européenne qui cherche à imposer à États tiers des restrictions sur les mesures qu'ils peuvent prendre dans la défense de leur sécurité nationale alors qu'elle est incapable d'imposer ces mêmes restrictions à ses États membres. La High Court irlandaise demandait enfin quel était le niveau de protection requis d'un pays tiers dans le cadre de clauses contractuelles types et comment les juridictions nationales devaient évaluer ce niveau de protection pour s'assurer qu'il est conforme à ce qui est requis selon la Directive de 95 (puisque les demandes initiales de M. Schrems ont été effectuées avant l'entrée en vigueur du RGPD) et la Charte.

La Cour répond tout d'abord dans la droite ligne de sa jurisprudence que seules les dispositions du droit communautaire, y compris la Charte, doivent être utilisées pour apprécier le caractère adéquat de la protection offerte par un pays tiers, à l'exclusion des dispositions des droits nationaux, même de rang constitutionnel. Cependant, la Cour va plus loin que ce qui lui était posé et considère que dans le cadre de clauses contractuelles types, la juridiction qui juge de la légalité du transfert doit procéder à un examen de la législation du pays destinataire concernant les possibilités d'accès des autorités de ce pays sur les mêmes critères que ceux énoncés par l'article 45.2 pour l'octroi du statut de pays offrant un niveau de protection équivalent. Ceci n'est aucunement requis par la rédaction de l'article 46, qui requiert simplement, dans son premier alinéa, pour le transfert de données hors de l'Union européenne en utilisant les CCT, que les personnes concernées disposent de droits opposables et de voies de droit effectives. Même si en pratique la législation américaine telle qu'elle est analysée dans la décision autorisant le Safe Harbour ne satisfait pas ce critère, la différence entre ces deux critères et une analyse de la totalité du système juridique d'un Etat tiers est pourtant de taille.

L'analyse qui est faite par la Cour affaiblit considérablement les CTT puisque si la Cour a annulé une décision d'adéquation de la Commission bénéficiant à un pays tiers, elles ne peuvent plus être utilisées pour transférer des données vers ce pays tiers et si une décision d'adéquation de ce pays tiers existe, les CTT vers ce pays tiers peuvent néanmoins être contestées en même temps que la décision d'adéquation. S'il n'existe pas de décision d'adéquation, l'autorité de contrôle doit procéder à sa propre analyse du système juridique du pays tiers et peut, si elle estime qu'il ne permettrait pas au pays d'obtenir une décision d'adéquation (la décision visant expressément l'article 45 du RGPD), interrompre le transfert de données.

Concrètement, il semble que les CCT suite à cette décision ne peuvent être utilisées pour transférer des données que vers de très rares pays dans le monde. Tout d'abord, il semble quasi certain que les Etats non démocratiques, où le respect de l'état de droit n'est pas assuré, ne peuvent pas accueillir de données personnelles en provenance de l'Union européenne, en l'absence de droit de recours effectif et de droits opposables. Les Etats pleinement démocratiques devront eux faire l'objet d'une analyse très détaillée et on peut s'interroger sur la marge de manœuvre existant concernant les démocraties dites illibérales, comme par exemple les Philippines.

Selon le Wall Street Journal[8], suite à cette décision, le Data Protection Commissionner dont la décision n'a pas été rendue publique a enjoint à Facebook de cesser tout transfert de données vers les Etats-Unis sur la base de ses CCT. Ceci est la suite logique de l'arrêt de la CJUE, aux termes duquel on ne voit pas selon quel mécanisme les transferts de données vers les États-Unis peuvent continuer. Le Comité européen de la protection des données et la Commission européenne ont chacun effectué des propositions pour permettre la continuité du transfert de données.

Les recommandations du CEPD

Le 10 novembre 2020, le CEPD a émis des recommandations sur les mesures qui complètent les outils de transfert pour assurer le respect du niveau européen de protection des données personnelles[9]. Malheureusement, ces recommandations sont d'une portée pratique très limitées. Elles sont divisées en 6 étapes, dont les deux premières assez évidentes : connaître ses flux géographiques de données et identifier si les pays peuvent bénéficier d'une décision d'adéquation. Dans ce premier cas, il n'y a effectivement aucun besoin de conclure des CCT.

La troisième étape requiert d'évaluer si des éléments dans la loi de l'état tiers ou dans la pratique de ses autorités pourrait constituer un obstacle à l'effectivité des CCT. Cette étape existe déjà dans les trois jeux de CCT proposés par la Commission européenne, qui font peser cette obligation sur l'importateur de données en lui faisant garantir qu'il n'a « *aucune raison de croire que la législation le concernant l'empêche de remplir les instructions données par l'exportateur de données et les obligations qui lui incombent conformément au contrat, et si ladite législation fait l'objet d'une modification susceptible d'avoir des conséquences négatives importantes pour les garanties et les obligations offertes par les clauses, il communiquera la modification à l'exportateur de données sans retard après en avoir eu connaissance, auquel cas ce dernier a le droit de suspendre le transfert de données et/ou de résilier le contrat* ».

D'un point de vue pratique, il semble logique que cette obligation pèse sur l'importateur de données, ne serait-ce que pour des raisons linguistiques. Cependant, le CEPD, suivant le raisonnement de la Cour, fait porter cette obligation sur l'exportateur de données. Afin d'assister l'exportateur de données dans cette analyse, le CEPD a émis une recommandation sur les quatre garanties essentielles pour les mesures de surveillances[10].

Ces garanties concernant les traitements de données européennes importées par les autorités de sécurité des Etats tiers sont :

- le traitement doit être basé sur des règles claires, précises et accessibles ;
- la nécessité de ces traitements et leur proportionnalité au regard de leur objectif légitime doit être démontrée ;
- un mécanisme de supervision indépendant doit exister ;
- des recours effectifs doivent être à la disposition des personnes européennes concernées.

Comme nous l'avons exposé ci-dessus, en réalité, il semble probable que l'examen de la législation de la plupart des Etats membres concernant l'accès aux données personnelles de ressortissants étrangers, pour des raisons de sécurité, démontrerait qu'aucun d'entre eux ne répond à ces critères. Ceci est en tous cas établi pour la France et la Belgique, qui ne font preuve à notre connaissance d'aucun zèle pour modifier leur législation suite à l'arrêt Quadrature du Net cité ci-dessus.

Cette demande d'analyse de la législation de pays situés à l'autre bout du monde semble assez irréaliste. On voit en effet mal comment une société française, ou un cabinet spécialisé en la matière, accepterait d'exposer sa responsabilité en analysant la législation concernant l'accès aux données personnelles étrangères par les autorités de l'Uttar Pradesh ou de Taïwan (pour prendre des Etats ou des régions démocratiques) lorsque la Commission européenne, avec tous les moyens dont elle dispose, se montre de manière répétée incapable d'analyser le niveau de conformité d'un pays de langue anglaise avec un système juridique qui est, quoi qu'on puisse en dire, très proche de celui de certains Etats membres. Le résultat de l'analyse de chaque pays au vu de ces critères sera probablement qu'il est impossible d'y transférer des données personnelles en utilisant le mécanisme des CCT. La seule solution pratique serait de demander aux autorités de contrôle de procéder à une telle analyse, afin d'indiquer vers quels pays le transfert de données par le mécanisme de SCC est possible, mais on constate qu'au vu de l'ampleur de la tâche, aucune autorité ne semble se porter volontaire.

La quatrième étape, si l'analyse démontre que la législation du pays concerné ne permet pas de transfert des données de façon sécurisée, serait d'adopter des mesures supplémentaires, au cas par cas et bien évidemment sous la responsabilité de l'exportateur de données. Le CEPD propose dans une annexe de 16 pages des exemples de mesures possibles qui vont toutes vers la dépersonnalisation des données, par l'anonymisation, la pseudonymisation ou le cryptage des données transférées. Néanmoins à part ces mesures techniques, aucun moyen juridique contractuel ne semble véritablement opposable à la réglementation d'un pays tiers prévoyant l'accès aux données transférées par ses autorités en charge de la sécurité nationale. Le CEPD a effectué une analyse très poussée de tous les moyens juridiques disponibles, mais on ne peut que constater qu'un contrat entre deux parties ne peut pas prévaloir sur la loi d'un Etat souverain, ce qui n'est pas véritablement surprenant.

Si des mesures supplémentaires sont envisageables, ce qui ne concernera en pratique qu'un nombre très limité de cas, la cinquième étape consiste en l'adoption des étapes procédurales pour mettre en place ces mesures supplémentaires. Si les CCT doivent être modifiées pour mettre en place ces mesures supplémentaires, l'exportateur de données doit obtenir l'autorisation de son autorité de contrôle, en application de l'article 46.3 du RGPD, puisqu'il ne fonde plus son transfert de données hors de l'Union européenne sur les CCT approuvées par la Commission.

La sixième étape consiste en une réévaluation régulière de la législation de l'Etat vers lequel les données sont transférées.

DOCTRINE

Les nouvelles CCT proposées par la Commission européenne

La Commission européenne a publié le 12 novembre dernier un nouveau projet de clauses contractuelles types, qui regroupe en un seul modèle les divers cas de figure de transfert de données hors de l'Union européenne, améliorant ainsi les clauses contractuelles types concernant les cas de transfert déjà couverts par des CCT (transferts de responsable à responsable et transferts de responsable à sous-traitant) mais aussi créant des CCT pour des cas non encore couverts par des CCT (transfert de sous-traitant à sous-traitant et transfert de sous-traitant à responsable), ce qui serait une amélioration considérable de ce mécanisme s'il pouvait encore avoir une quelconque utilité après l'arrêt Schrems II.

Les articles 2 et 3 de ces nouvelles CCT, communs à tous les cas de figure, essaient de traiter cette question, sans malheureusement y parvenir de façon vraiment satisfaisante. Selon les termes de l'article 2 de ces nouvelles CCT, les parties garantissent qu'elles n'ont aucune raison de croire que la législation de l'Etat tiers, et en particulier celle concernant l'accès aux données par les autorités publiques de cet Etat tiers, empêcherait l'importateur de données de respecter ces obligations au titre des CCT. Cette évaluation, qui doit être effectuée selon des critères nombreux et très détaillés, doit être documentée par les parties et communicable aux autorités de contrôle. Comme nous l'avons vu précédemment, ceci requiert une analyse que peu d'exportateurs et d'importateurs de données sont capables d'effectuer. L'importateur de données doit notifier à l'exportateur tout changement affectant cette réglementation, qui doit dans ce cas prendre toute mesure supplémentaire appropriée en les notifiant à l'autorité de contrôle et au responsable de traitement, le cas échéant. La clause 3 prévoit que l'importateur de données doit immédiatement notifier à l'exportateur de données, s'il en a le droit, toute demande d'accès aux données de la part des autorités nationales ou tout accès aux données par ces autorités dès qu'il en aurait connaissance. S'il n'a pas le droit de transmettre ces informations à l'exportateur de données, l'importateur de données doit faire ses meilleurs efforts pour l'obtenir. S'il n'arrive pas à obtenir ce droit, le dernier alinéa implique qu'il doit alors informer l'exportateur de données que la législation de son pays ne lui permet plus de respecter les CCT.

Au vu de ces deux propositions, quatre mois après la décision Schrems 2, aucune solution satisfaisante pour transférer en toute sécurité juridique des données personnelles hors de l'Union européenne ne semble se présenter. Les CCT ne peuvent plus être utilisées pour transférer de façon pleinement sécurisée des données hors de l'Union européenne que vers un nombre probablement très limité de pays. On constatait déjà depuis un certain nombre d'années un mouvement général de relocalisation des centres de données vers les pays de l'Union européenne, mais la décision Schrems 2 va certainement accélérer ce mouvement.
Cependant, les transferts de données entre l'Union européenne et le reste du monde demeurent un élément nécessaire du commerce mondial et une frontière absolument étanche entre l'Union européenne et le reste du monde, où les données personnelles ne pourraient être exportées que sur la base très étroite des dérogations pour des situations particulières prévues à l'article 49 du RGPD. Ce qui ne semble ni désirable, ni même possible, au vu de l'interconnexion du monde dans lequel nous vivons. On ne peut que constater l'impasse dans laquelle cette décision Schrems II a conduit aussi bien les autorités nationales et européennes que les responsables de traitement, qui reflète en fait les tensions, aussi bien à l'intérieur qu'à l'extérieur de l'Union européenne entre la demande légitime de respect de chaque souveraineté nationale et les besoins des échanges internationaux, avec les améliorations réelles au niveau de vie des citoyens qu'ils impliquent, lorsqu'ils ne se limitent plus aux marchandises mais concernent de plus en plus des services et des biens dématérialisés.

Marc LEMPERIERE
Avocat associé
ALMAIN

Notes

(1) CJUE, Data Protection Commissioner c/ Facebook Ireland Ltd et Maximilian Schrems, 16 juillet 2020, C-311/18

(2) CJUE, Maximillian Schrems c/ Data Protection Commissioner, 8 octobre 2015, C-362/14

(3) Charte des droits fondamentaux de l'Union européenne, 2016/C 202 02

(4) Décision de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil (n° C(2010) 593)

(5) The High Court , Commercial, The Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, 2016 n°4809 P)

(6) Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-Etats-Unis

(7) CJUE, affaires jointes C-511/18 et C-520/18, 6 octobre 2020

(8) Wall Street Journal, 9 septembre 2020, "Ireland to order Facebook to stop sending users data to US", Sam Schechner et Emilie Glazer

(9) EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

(10) EDPB, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures

Vous avez envie de vous exprimer sur un sujet qui vous tient à cœur, de partager votre analyse avec la communauté des lecteurs d'Expertises, d'exposer un point de vue différent sur un article déjà publié, de lancer un débat sur un thème émergent, ou simplement de commenter l'actualité du droit du numérique ?

Contactez la rédactrice en chef d'Expertises Sylvie Rozenfeld sr@expertises.info