BANQUE DES MEMOIRES

Master de droit du Numérique
Dirigé par Monsieur le Professeur Jérôme Passa
2021

Lois de surveillance et protection des données personnelles

Ou une analyse de l'arrêt Schrems II

Mahaut Mermet

Sous la direction de Maître Lorraine Maisnier-Boché

Année universitaire 2020/2021

Lois de surveillance et protection des données personnelles

Ou une analyse de l'arrêt Schrems II

Mémoire présenté pour l'obtention du Master II par **Mahaut Mermet**

Sous la direction de **Maître Lorraine Maisnier-Boché**

Dans le cadre du M2 de droit du numérique de Paris II Panthéon-Assas, dirigé par **Monsieur Le Professeur Jérôme Passa**

Remerciements

Je tiens à remercier tout d'abord Maître Lorraine Maisnier-Bosché pour la direction de ce mémoire et pour ses précieux conseils.
Je remercie aussi mes correcteurs, mes amis et ma famille pour leurs justes remarques et leur encouragement.

Un grand merci aussi à Monsieur le Professeur Jérôme Passa pour m'avoir permis de passer cette année en M2 de droit du Numérique à Assas sous sa direction et ainsi de faire ce mémoire.

Principales abréviations

Art.	Article
RGPD	Règlement général sur la protection des données
CE	Conseil d'État
Cons. Const.	Conseil constitutionnel
Conv EDH	Convention européenne des droits de l'Homme
CEDH	Cour européenne des droits de l'Homme
CJUE	Cour de justice de l'Union européenne
CNIL	Commission nationale de l'informatique et des libertés
aff.	Affaire
Com., Com, élec.	Revue « Communication Commerce Électronique »
comm.	Commentaire
D.	Recueil Dalloz
Dalloz IP IT	Revue Dalloz droit des nouvelles technologies de l'information et de la communication
éd.	Edition
In	Dans
LGDJ	Librairie générale de droit et de jurisprudence
n°	Numéro
Obs.	Observations
Op. cit.	Ouvrage cité
p.	Page
Rapp.	Rapport
RTD eur.	Revue trimestrielle de droit européen
AJDA	Actualité juridique Droit administratif
Gaz. pal.	Gazette du Palais
Rev. UE	Revue de l'Union Européenne
v.	Voyez
APPI	loi sur la protection des informations à caractère personnel japonaise
PPC	Commission de protection des données personnelles japonaise

Sommaire

"J'ai cessé d'ignorer à l'âge de trois ou quatre ans et parfois ça me manque" (Romain Gary - La vie devant soi)

Introduction

Le 16 juillet 2020, la fameuse décision Schrems II a invalidé le mécanisme du "privacy shield" qui permettait de transférer des données européennes aux Etats-Unis sans plus de formalités[1]. La Cour de Justice de l'Union Européenne s'est fondée sur le fait que la réglementation aux Etats-Unis n'accordait pas une protection adéquate des personnes dont les données étaient transférées, et cela notamment du fait de lois de surveillance très intrusives. Le Foreign Intelligence Surveillance Act (FISA) de 1978 et l'Executive Order (E.O.) 12333 de 1981 ont été cité dans l'affaire pour montrer que les autorités de surveillance américaines avaient la possibilité de recueillir massivement des données, y compris européennes.[2] Cet arrêt fait suite à l'arrêt Schrems 1 de 2015 qui a invalidé le système de "safe Harbor", dont l'objet était le même que le "Privacy Shield", notamment sur la base de l'affaire "Prism" et du fait de la surveillance généralisée engendrée, qui ne permettait pas d'assurer une protection adéquate des données.[3]

Ce n'est pas la première fois qu'un système de surveillance fait l'objet de controverses, ce n'est pas non plus le seul pays concerné par ces critiques et ces condamnations de la cour de justice de l'Union Européenne. En France par exemple, la loi du 24 juillet 2015 modifiée en 2016, qui donnait un cadre légal aux services de renseignement, a entraîné une levée de boucliers. Les critiques s'attachaient à dénoncer des définitions larges qui donnent une capacité d'interprétation trop grande au gouvernement, une surveillance internationale jugée excessivement importante et sans garantie appropriée,[4] et la possibilité donnée aux services de renseignement de collecter les données de connexion des personnes considérées comme menaçantes pour la sécurité publique.[5] Cette législation française a été

[1] Commission européenne, UE-US Privacy Shield, 2 février 2016
[2] Arrêt "Schrems 2", la cour de justice de l'Union Européenne invalide le système du privacy shield - Par Sophie Haddad, Antoine Casanova, Nina Dubois, Avocats - le 7 août 2020 - Village Justice
[3] C-362/14 - Schrems - Arrêt de la CJUE , grande chambre, du 6 octobre 2015 - point 22 de l'arrêt
[4] Loi Renseignement : la surveillance internationale examinée par les députés le 1er octobre - Marc Rees - Nextinpact - 21/09/2015
[5] La justice européenne s'oppose à la transmission et la conservation généralisée des données de connexion - Source : L'usine digitale - Alice Vitard - 06/10/2020

indirectement condamnée par la CJUE dans un arrêt Télé2 Sverige de 2016[6] ; puis plus récemment, la cour de justice[7] a directement statué sur l'illégalité des pratiques de conservation « généralisée et indifférenciée » des données de connexion mises en place par le droit français dans le cadre de son système de surveillance, notamment contre le terrorisme, au regard de la protection des données personnelles.[8]

Les définitions ne sont pas un point à négliger que ce soit dans une loi, dans un contrat, dans un règlement et même dans un mémoire. Ainsi il est important tout d'abord de bien avoir à l'esprit ce que veulent dire les mots " surveillance", "sécurité" et "données à caractère personnel". Il n'y a pas de définition légale de la surveillance dans sa terminologie générale. Le Centre national de ressources textuelles et lexicales (CNRTL) la définit comme "*l'action ou le fait de surveiller une personne dont on a la responsabilité ou à laquelle on s'intéresse*", ou encore comme "l*'activité policière consistant à surveiller des personnes suspectes ou des milieux à risques, pour prévenir des actions délictueuses ou criminelles, pour garantir la sécurité publique*." Cette dernière est considérée en droit français par l'article L 111-1 du code de la sécurité intérieure comme « *un droit fondamental et l'une des conditions de l'exercice des libertés individuelles et collectives* ». C'est plus précisément, selon la suite de l'article, le fait pour l'Etat de veiller sur l'ensemble du territoire de la République, de défendre les institutions et les intérêts nationaux, le respect des lois, le maintien de la paix et de l'ordre public, ainsi que de protéger les personnes et les biens[9]. On voit ici que la surveillance et la sécurité sont extrêmement liées, puisque dans la notion de sécurité il y a la notion de "veiller sur" le maintien de la paix afin de mettre les citoyens à l'abri de tout danger. La sécurité civile quant à elle est différente, l'article L 112-1 du même code de la sécurité intérieure le précise, car elle n'a pour objet que "*la prévention des risques de toute nature, l'information et l'alerte des populations ainsi que la protection des personnes, des biens et de l'environnement contre les accidents, les sinistres et les catastrophes par la préparation et la mise en œuvre de mesures et de moyens appropriés relevant de l'Etat, des collectivités territoriales et des autres personnes publiques ou privées*". La lutte contre le terrorisme et contre la délinquance définie comme tout crime et délit selon

[6] CJUE (grande chambre) 21 décembre 2016, affaires jointes C-203/15 et C-698/15, Tele2 Sverige AB contre Post- och telestyrelsen et Secretary of State for the Home Department contre Tom Watson e.a.
[7] Décision La Quadrature du Net e.a., affaires jointes C-511/18 et C-512/18 et Ordre des barreaux francophones et germanophone e.a., C-520/18 du 6 octobre 2020 ;
[8] Liste des données à conserver données dans l'article R. 10-13 du CPCE - Décision La Quadrature du Net e.a., affaires jointes C-511/18 et C-512/18 et Ordre des barreaux francophones et germanophone e.a., C-520/18 du 6 octobre 2020 - point 47
[9] Article L111-1 du code de la sécurité intérieure

l'article L 132-2 du code de la sécurité intérieure ne font pas partie de cette dernière définition, il s'agit en effet ici de protection de l'environnement, de sécurité routière etc. Seule la sécurité publique intéressera les propos qui vont suivre et non pas la sécurité civile.

Pour surveiller il est nécessaire de faire appel à la notion de renseignement, qui désigne la collecte d'informations stratégiques sur une personne, une institution, ou encore une technologie. Le terme renvoie aussi aux services qui recueillent les informations nécessaires à identifier et prévenir toute menace susceptible de porter atteinte à la sécurité d'un État.[10] Or toute "information", "*dès lors qu'elle permet d'identifier nominativement une personne physique ou même seulement de la rendre identifiable, voire simplement de la singulariser*"[11] est soumise au principe fondamental de protection des données personnelles.

Ainsi, pour établir un système de surveillance, il est nécessaire de passer par des traitements d'informations stratégiques, et donc souvent de données personnelles. Une donnée personnelle est définie dans l'article 4 du RGPD comme "toute information se rapportant à une personne physique identifiée ou identifiable"[12], c'est une donnée qui permet d'identifier directement ou indirectement la personne à qui elle se rapporte (donnée de localisation, identifiant etc.). La protection de ces données entre dans le champ des droits fondamentaux[13] au même titre que la protection de la vie privée, et même "à l'aune du droit au respect de la vie privée".[14] Partant, l'Union Européenne "*appréhende et protège les données à caractère personnel et le droit à la vie privée du point de vue des droits fondamentaux, notamment aux articles 7 et 8 de la Charte des droits fondamentaux de l'UE,*

[10] Source : site de Vie publique, "Renseignement français : quelle organisation et quel cadre légal ?", publié le 15 janvier 2020

[11] Source : LexisNexis - Fasc. 274-10 : Informatique . – Données à caractère personnel . – Introduction générale et champ d'application de la réglementation relative à la protection des données personnelles - point clé n°8 / Date du fascicule : 9 Avril 2019 / Date de la dernière mise à jour : 28 Février 2021/ Auteurs : Romain Perray - Avocat associé – McDermott Will & Emery AARPI - Chargé d'enseignement à l'université de Paris I – Panthéon-Sorbonne, à l'Université de Paris II – Panthéon-Assas, à l'Université de Paris V – Paris-Descartes

[12] Article 4.1 RGPD

[13] Article 8 Charte des droits fondamentaux de l'Union Européenne - Protection des données à caractère personnel : 1. Toute personne a droit à la protection des données à caractère personnel la concernant.2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.

[14] "La protection des données personnelles à l'aune du droit au respect de la vie privée et familiale de l'article 8 de la convention" - Base Lextenso - Gaz. Pal. 3 déc. 2019, n° 364m9, p. 15 - Auteurs : Jean-Luc Sauron, conseiller d'État, professeur associé à l'université Paris Dauphine, Mattias Guyomar, conseiller d'État, professeur associé de droit public à l'université Panthéon-Assas (Paris 2)

l'article 16, paragraphe 1 du TFUE, l'article 8[15] *de la Conv EDH ainsi que la Convention du Conseil de l'Europe n° 108*."[16] Cependant, en ce qui concerne la protection et la prévention des infractions pénales et contre les menaces pour la sécurité publique, celle des données personnelles est assouplie pour donner plus de marge de manœuvre aux autorités assurant cette sécurité, du fait de la directive Police Justice de 2016.[17] Les traitements mis en œuvre pour assurer la sûreté de l'Etat ou encore la défense nationale ne relèvent pas du champ d'application de l'Union européenne et restent régis par les dispositions de la seule loi « Informatique et Libertés » et notamment l'article 31 de la loi.[18]

L'enjeu ici, finalement, est la proportionnalité entre deux droits fondamentaux : la liberté (passant par la vie privée et la protection des données) et la sécurité. "*La liberté, ce bien qui fait jouir des autres biens*" disait Montesquieu. Car tout comme la sécurité, la liberté permet de profiter des autres droits fondamentaux. Ainsi il est toujours délicat de savoir où placer la limite entre ce qu'il est possible de faire pour la sécurité d'une société et ce qu'il est nécessaire de sauvegarder en vertu de la liberté et du droit au respect de la vie privée de l'article 9 du code civil et 8 de la convention européenne des droits de l'homme. Cet enjeu se pose dans de nombreux domaines. Par exemple, est ce que pour protéger l'intégrité de la personne humaine et le maintien de la paix on peut interdire de publier tout propos à caractère raciste, sexiste, pédo-pornographique, terroriste etc. et donc "surveiller" ce qui se dit sur les réseaux et limiter la liberté d'expression ? ou vaut-il mieux garder une liberté d'expression sans limite et donc risquer de laisser des propos condamnables circuler ? C'est la

---

[15] Article 8 Conv EDH "Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

[16] Répertoire de droit européen - Économie collaborative : vers un cadre de la régulation des plateformes ? – Économie collaborative et perturbation des taxonomies juridiques traditionnelles – Vassilis HATZOPOULOS – Janvier 2020 (actualisation : Octobre 2020) - chap. 1 ; sect. 3 ; art. 3 ; 41 - Source : Dalloz

[17] Dir. UE 2016/680 du Parlement européen et du Conseil du 27 avril 2016 - Considérant 4 : "*Il convient de faciliter le libre flux des données à caractère personnel entre les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces au sein de l'Union, et le transfert de telles données vers des pays tiers et à des organisations internationales, tout en assurant un niveau élevé de protection des données à caractère personnel. Ces évolutions obligent à mettre en place dans l'Union un cadre pour la protection des données à caractère personnel solide et plus cohérent, assorti d'une application rigoureuse des règles.*"

[18] Source CNIL : Directive « Police-Justice » : de quoi parle-t-on ?- 20 février 2019

problématique qui s'est posée dans la directive du 8 juin 2000[19] transposé par la LCEN du 21 juin 2004[20], dans l'arrêt de la CJUE du 6 octobre 2020[21] sur la compatibilité des algorithmes de surveillance autorisés par la loi Renseignement de 2015 avec la charte des droits fondamentaux ou encore dans le projet de loi Avia censuré en grande partie par le Conseil Constitutionnel le 18 juin 2020[22] au motif que ce projet portait trop fortement atteinte à la liberté d'expression.

La CJUE est évoquée car la problématique n'est pas simplement nationale, elle est européenne[23], ainsi que la Cour EDH qui est importante en la matière car elle vise à protéger les droits et libertés fondamentales des Etats signataires[24]. De là, la Convention européenne des droits de l'Homme[25], la charte des droits fondamentaux de l'union européenne[26], la directive police-justice[27] et le RGPD[28], transposés en France dans la loi informatique et liberté[29], viennent protéger les données des personnes concernées par la mise en place d'un cadre juridique adéquat concernant tout traitement[30] et transfert de données en dehors de l'Union européenne, etc. Un transfert de données faisant référence à *"toute communication, copie ou déplacement de données personnelles ayant vocation à être traitées dans un pays tiers à l'Union européenne*"[31]. On voit donc que cela devient une problématique aussi internationale, faisant entrer notamment des enjeux de transferts de données et donc de protection essentiellement équivalente dans les pays vers lesquels les données sont

[19] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»)
[20] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique
[21] C-511/18 - La Quadrature du Net e.a.
[22] Décision n° 2020-801 DC du 18 juin 2020
[23] L'application du RGPD et de la Directive Police Justice le montre bien
[24] CEDH Klass et autres c. Allemagne (Req. 5029/71), 6 septembre 1978 / CEDH, Roman Zakharov c. Russie [GC], n° 47143/06, 4 décembre 2015 / CEDH Szabo et Vissy c. Hongrie (Req. 37/138/14), 12 janvier 2016
[25] Article 8 Conv EDH notamment
[26] Article 7, 8, 52§1 CDF
[27] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil
[28] 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).
[29] Loi no 78-17 du 6 janvier 1978
[30] Article 4. 2 RGPD : «traitement», toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction
[31] Définition du transfert de données de la CNIL

transférées. Il est alors nécessaire de tenir compte des lois de surveillance qui sont édictées dans les pays tiers pour accepter un transfert de données et jauger de la sécurité à mettre en place autour du transfert pour que les données européennes soient protégées dans un pays non européen[32]. Mais cela soulève de nombreuses questions, tout d'abord dans quelle mesure il est possible d'être sûr de la non-ingérence d'un Etat tiers qui voudrait préserver ses intérêts lors d'un transfert de données ? Comment concilier sécurité publique et préservation de la vie privée et protection des données personnelles ?

A ce titre, il est intéressant de noter que l'arrêt Schrems II[33] a apporté certaines pistes de réflexion et certains critères pour étudier la protection entourant des données lors d'un transfert et plus largement pour étudier la protection entourant les données face aux lois de surveillance de tout Etat. L'analyse qui va suivre se focalisera surtout sur la portée de l'arrêt Schrems II, son analyse du RGPD et du droit à la protection des données personnelles, et ses conséquences sur l'adéquation des lois de surveillance au droit fondamental de protection des données personnelles. L'arrêt sera mis en relation avec la réglementation et la jurisprudence françaises et européennes.

L'arrêt Schrems II sonne-t-il le glas de l'exposition des données personnelles et de la vie privée à la surveillance des Etats ?

Pour répondre à cette problématique, le critère de la cohérence apportée par l'arrêt Schrems II sera tout particulièrement étudié pour montrer que la protection des données se renforce de plus en plus (partie I). Ensuite il s'agira de voir qu'en pratique il est encore difficile de faire respecter la cohérence et la protection effective des données face à la surveillance des Etats (partie II).

[32] Article 44 RGPD et suivants
[33] CJUE 16 juillet 2020, Arrêt Schrems II, aff. C-311/18

Partie 1 : La protection des données à l'aune de sa cohérence

Il est intéressant d'étudier cette volonté de cohérence générale dans la réglementation qu'a voulu mettre en lumière l'arrêt Schrems II (section 1) pour l'appliquer aux transferts de données (section 2).

Le critère de la cohérence retenu dans l'arrêt Schrems II, un prisme pour analyser l'état de la protection des données personnelles face aux lois de surveillance

Section 1 : La consécration d'un critère de cohérence

M. Maximilian Schrems est un ressortissant autrichien qui a déposé une plainte auprès de l'autorité de contrôle irlandaise pour faire interdire les transferts de Facebook Ireland vers les serveurs de Facebook Inc. situés aux Etats-Unis car ceux-ci n'offrent pas une sécurité des données adéquates[34]. Sa demande a d'abord été rejetée par la commission dans une décision 2000/520[35]. Mais la cour de justice de l'Union Européenne a jugé cette décision invalide dans le fameux arrêt Schrems I[36] et en conséquence le système du "Safe Harbor" a été invalidé. Par la suite une nouvelle convention a été signée, nommée "Privacy Shield"[37], pour assurer une protection des données personnelles conforme aux attentes de la réglementation européenne. M. Schrems a donc une nouvelle fois attaqué cette décision au motif que les lois de surveillance américaines ne permettent pas d'assurer une protection suffisante de ces données. La Cour de Justice de l'Union Européenne a de nouveau accueilli l'argument, invalidé le "*Privacy Shield*" et contraint les transferts de données européennes vers les Etats-Unis. Une autre décision était mise en cause dans cette affaire, la décision 2010/87, sur

[34] CJUE C-362/14,6 octobre 2015, Schrems - Point 52 : Le 25 juin 2013, M. Schrems a saisi le commissaire d'une plainte par laquelle il demandait, en substance, à celui-ci d'interdire à Facebook Ireland de transférer ses données à caractère personnel vers les États-Unis, en faisant valoir que le droit et les pratiques en vigueur dans ce pays ne garantissaient pas une protection suffisante des données à caractère personnel conservées sur le territoire de celui-ci contre les activités de surveillance qui y étaient pratiquées par les autorités publiques. Cette plainte a été rejetée, au motif, notamment, que la Commission avait constaté, dans sa décision 2000/520, que les États-Unis assuraient un niveau adéquat de protection

[35] Décision de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique (JO 2000, L 215, p. 7).

[36] Arrêt de la Cour du 6 octobre 2015, Schrems, C-362/14 (voir également CP no 117/15)

[37] Décision d'exécution 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 (JO 2016, L 207, p. 1).

la validité des clauses contractuelles types pour assurer une protection adéquate lors d'un transfert de données, mais la cour de justice a considéré qu' "*au regard de la charte des droits fondamentaux de l'Union européenne*" elle "*ne révèle aucun élément de nature à affecter sa validité.*"[38] Ainsi la possibilité de passer par des clauses contractuelles types pour fonder un transfert de données est restée en vigueur.

Pour fonder sa solution, le juge s'est appuyé sur un critère de cohérence dans la protection des données personnelles (A) et a pu lire, à partir de là, les critères déjà connus à l'aune de ce nouveau critère de continuité et de cohérence dans la protection. (B)

A. Une cohérence dans le temps et dans l'espace

La décision Schrems II est loin de se limiter à l'invalidation du Privacy Shield et à la reconnaissance de la validité des clauses contractuelles types ; elle a aussi permis à la Cour de donner des précisions intéressantes concernant la protection des données personnelles, " *sur l'applicabilité ratione temporis et ratione loci du RGPD"*[39] ainsi que, et c'est lié, sur la cohérence de fond qu'elle veut donner à la matière grâce à l'application cumulée du RGPD et de la Charte des droits fondamentaux.

Le RGPD a pu être appliqué au cas d'espèce, pour un acte passé antérieurement à l'entrée en vigueur du règlement, le Privacy Shield.[40] Cela signifie que les dispositions du RGPD sont considérées comme trop importantes pour être mises de côté et donc qu'il est possible de s'affranchir du principe de sécurité juridique de non-rétroactivité de la loi nouvelle.[41] Ce principe n'est un droit fondamental protégé par le droit européen qu'en matière

[38] Cour de justice de l'Union européenne communiqué de presse n° 91/20 Luxembourg, le 16 juillet 2020 Arrêt dans l'affaire C-311/18 Data Protection Commissioner/Maximillian Schrems et Facebook Ireland
[39] Revue de l'Union européenne - L'arrêt Schrems II, vers une résolution de l'équation transatlantique ? – Alexis Deroudille – Rev. UE 2021. 144
[40] Arrêt Schrems II - C-311/18 - Point 79 : "*Dès lors, il y a lieu de répondre aux questions préjudicielles au regard des dispositions du RGPD, et non de celles de la directive 95/46."*
[41] Article 2 du code civil : *"la loi ne dispose que pour l'avenir ; elle n'a point d'effet rétroactif*"

pénale[42], cependant il existe un droit au procès équitable[43] selon lequel " Toute personne a droit à ce que sa cause soit entendue équitablement".[44] Un aspect du procès équitable est d'être jugé par rapport à une législation qui était en vigueur au moment des faits litigieux. Or ici le RGPD s'est tout de même appliqué, certainement car la protection des données est un principe fondamental[45] et à ce titre c'est une réglementation fondamentale qui ne peut être mise de côté. La question s'est aussi posée de savoir si le Règlement de Protection des Données Personnelles pouvait s'appliquer alors que la sécurité publique de l'Etat tiers est en cause et que le règlement, tout comme l'ancienne directive 95/46/CE, exclut de son champ d'application la protection de la sécurité publique, [46] par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la

[42] Article 49 Charte des droits fondamentaux de l'Union Européenne : 1. Nul ne peut être condamné pour une action ou une omission qui, au moment où elle a été commise, ne constituait pas une infraction d'après le droit national ou le droit international. De même, il n'est infligé aucune peine plus forte que celle qui était applicable au moment où l'infraction a été commise. Si, postérieurement à cette infraction, la loi prévoit une peine plus légère, celle-ci doit être appliquée. 2. Le présent article ne porte pas atteinte au jugement et à la punition d'une personne coupable d'une action ou d'une omission qui, au moment où elle a été commise, était criminelle d'après les principes généraux reconnus par l'ensemble des nations. 3. L'intensité des peines ne doit pas être disproportionnée par rapport à l'infraction.

[43] Article 6 CEDH : Toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable, par un tribunal indépendant et impartial, établi par la loi, qui décidera, soit des contestations sur ses droits et obligations de caractère civil, soit du bien-fondé de toute accusation en matière pénale dirigée contre elle. Le jugement doit être rendu publiquement, mais l'accès de la salle d'audience peut être interdit à la presse et au public pendant la totalité ou une partie du procès dans l'intérêt de la moralité, de l'ordre public ou de la sécurité nationale dans une société démocratique, lorsque les intérêts des mineurs ou la protection de la vie privée des parties au procès l'exigent, ou dans la mesure jugée strictement nécessaire par le tribunal, lorsque dans des circonstances spéciales la publicité serait de nature à porter atteinte aux intérêts de la justice. 2.Toute personne accusée d'une infraction est présumée innocente jusqu'à ce que sa culpabilité ait été légalement établie. 3. Tout accusé a droit notamment à:

- être informé, dans le plus court délai, dans une langue qu'il comprend et d'une manière détaillée, de la nature et de la cause de l'accusation portée contre lui;
- disposer du temps et des facilités nécessaires à la préparation de sa défense;
- se défendre lui-même ou avoir l'assistance d'un défenseur de son choix et, s'il n'a pas les moyens de rémunérer un défenseur, pouvoir être assisté gratuitement par un avocat d'office, lorsque les intérêts de la justice l'exigent;
- interroger ou faire interroger les témoins à charge et obtenir la convocation et l'interrogation des témoins à décharge dans les mêmes conditions que les témoins à charge;
- se faire assister gratuitement d'un interprète, s'il ne comprend pas ou ne parle pas la langue employée à l'audience.

[44] Article 47 CDFUE : Toute personne dont les droits et libertés garantis par le droit de l'Union ont été violés a droit à un recours effectif devant un tribunal dans le respect des conditions prévues au présent article. Toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable par un tribunal indépendant et impartial, établi préalablement par la loi. Toute personne a la possibilité de se faire conseiller, défendre et représenter. Une aide juridictionnelle est accordée à ceux qui ne disposent pas de ressources suffisantes, dans la mesure où cette aide serait nécessaire pour assurer l'effectivité de l'accès à la justice.

[45] Article 8 Charte des droits fondamentaux de l'Union Européenne

[46] Article 2, 2 D - "*Le présent règlement ne s'applique pas au traitement de données à caractère personnel effectué (...) par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces*."

sécurité publique et la prévention de telles menaces. La Cour répond et refuse que les traitements de données mis en œuvre par les agences gouvernementales américaines aux fins de sécurité publique et de protection contre les menaces terroristes bénéficient de ces exceptions. Le RGPD est ainsi applicable aux transferts de données originairement à des fins commerciales mais qui par la suite seront " *traitées par les autorités du pays tiers concerné à des fins de sécurité publique, de défense et de sûreté de l'État* »[47] (pts 80 à 89)[48]. Mais ce faisant elle ne justifie en rien le pourquoi d'une telle affirmation[49] et laisse un attendu de principe sans véritable fondement juridique selon Maître Deroudille. Cependant on pourrait aussi considérer que le fondement se trouve dans ce prisme de continuité de la protection des données qu'a voulu mettre en exergue la CJUE dans l'arrêt. En effet, cela pourrait être une certaine preuve de l'application de la cohérence dans la protection des données à caractère personnel que le RGPD se soit bien appliqué dans l'arrêt Schrems II car alors même qu'il s'agissait de traitements de données à des fins de surveillance et de sécurité publique, mais que tout d'abord ces données avaient été collectées à des fins commerciales, la protection n'est pas tombée. Ainsi, quand bien même dans la durée de vie de la donnée celle-ci est utilisée à des fins de surveillance[50], les règles de protection des données du RGPD s'appliquent car ce n'était pas le but premier du traitement de cette donnée qui avait vocation à rester dans la sphère commerciale. Le critère de continuité dans la vie des données passe au-dessus de la mise en œuvre de la sécurité publique et donc assure une plus grande sécurité des données personnelles, devenant finalement, presque, une nouvelle règle de protection.[51]

---

[47] Arrêt de la Cour (grande chambre) du 16 juillet 2020. Data Protection Commissioner contre Facebook Ireland Ltd et Maximillian Schrems.

[48] Transfert de données vers les USA : l'arrêt Schrems II AFFAIRES | Contrat - Responsabilité IP/IT ET COMMUNICATION | Contrat – Responsabilité | Protection des données Le très attendu arrêt « Schrems II » de la Cour de justice de l'Union européenne invalide, d'une part, le bouclier de protection des données dit Privacy Shield, mais considère comme valides, d'autre part, les clauses contractuelles types de la Commission européenne. par Cécile Crichton - le 22 juillet 2020 - CJUE 16 juill. 2020, DPC c. Facebook Ireland Ltd et M. Schrems, aff. C-311/18

[49] L'arrêt Schrems II, vers une résolution de l'équation transatlantique ? – Alexis Deroudille – Rev. UE 2021. 144

[50] Point 80 de l'arrêt : relève du champ d'application de ce règlement un transfert de données à caractère personnel effectué par un opérateur économique établi dans un État membre vers un autre opérateur économique établi dans un pays tiers, lorsque, au cours ou à la suite de ce transfert, ces données sont susceptibles d'être traitées par les autorités de ce pays tiers à des fins de sécurité publique, de défense et de sûreté de l'État.

[51] Arrêt Schrems II - C-311/18 - Points 88 et 89 - 88 : *"Il s'ensuit qu'un tel transfert ne saurait échapper au champ d'application du RGPD au motif que les données en cause sont susceptibles d'être traitées, au cours ou à la suite de ce transfert, par les autorités du pays tiers concerné, à des fins de sécurité publique, de défense et de sûreté de l'État*." 89 : "*Partant, il y a lieu de répondre à la première question que l'article 2, paragraphes 1 et 2, du RGPD doit être interprété en ce sens que relève du champ d'application de ce règlement un transfert de données à caractère personnel effectué à des fins commerciales par un opérateur économique établi dans un État membre vers un autre opérateur économique établi dans un pays tiers, nonobstant le fait que, au cours ou à la suite de ce transfert, ces données sont susceptibles d'être traitées par les autorités du pays tiers concerné à des fins de sécurité publique, de défense et de sûreté de l'État."*

Après avoir donné ces précisions sur l'application du RGPD, la Cour de Justice reste dans la logique amorcée en amont par l'arrêt Schrems I, même si le RGPD n'existait pas encore à l'époque, en réaffirmant le souci de faire primer la protection des données personnelles face aux lois de surveillance américaines. Et même si l'arrêt Schrems II est long et parfois redondant, une trame de fond demeure : la volonté d'ancrer et de ciseler cette "*conception constitutionnelle européenne de la protection des données*"[52]. Les Professeurs Brunessen et Sirinelli y voient une volonté de mettre en place une "cohérence" de fond au sujet de la réglementation protectionniste en matière de données et cela grâce à une utilisation courante et presque naturelle du RGPD sur les sujets lui offrant un terrain adéquat. "*Ce texte*" devant "*être lu, pensé, interprété comme un tout qui instaure une protection constitutionnelle européenne homogène et cohérente en dépit de la pluralité des régimes juridiques qu'il prévoit*".[53] En appliquant ainsi le RGPD pour un acte passé avant son entrée en vigueur et dans un cas qui pouvait à première vue tomber dans les exceptions de son article 2 mais qui, grâce à une interprétation extensive de la Cour a su s'imposer en l'espèce, le juge européen affirme la supériorité de ce principe de protection des données, lié intimement au droit fondamental de protection de la vie privée, sur les réglementations particulières. Finalement le RGPD devient une clé de lecture dès que des données personnelles sont en cause, dont les contours sont aussi à mettre en lien avec la Charte des droits fondamentaux de l'Union Européenne, puisque la Cour ne manque pas de rappeler dans son point 94 que l'étude de l'adéquation d'un pays tiers aux dispositions du RGPD doit se faire "à la lumière de la Charte"[54]. Il n'est pas question de se référer à l'article 8 de la Convention Européenne des Droits de l'Homme, le juge se contente ainsi des textes de l'Union européenne et affirme par là l'indépendance de l'ordre juridique de l'Union Européenne pour juger de ce cas. Le point 98 de l'arrêt ne vient que confirmer cette analyse.[55]

---

[52] Dalloz IP/IT - Schrems II : on prend les mêmes et on recommence – Brunessen Bertrand – Jean Sirinelli – Dalloz IP/IT 2020 - Page 640 - n°11 du 23/11/2020

[53] Transfert de données vers les USA : l'arrêt Schrems II AFFAIRES | Contrat - Responsabilité IP/IT ET COMMUNICATION | Contrat – Responsabilité | Protection des données Le très attendu arrêt « Schrems II » de la Cour de justice de l'Union européenne invalide, d'une part, le bouclier de protection des données dit Privacy Shield, mais considère comme valides, d'autre part, les clauses contractuelles types de la Commission européenne. par Cécile Crichton - le 22 juillet 2020 - CJUE 16 juill. 2020, DPC c. Facebook Ireland Ltd et M. Schrems, aff. C-311/18

[54] Plus précisément à ses article 7 et 8 et 47 (point 1 de l'arrêt Schrems II)

[55] CJUE 16 juillet 2020, Schrems II, C-311/18, point 98 : "*À cet égard, il convient de rappeler que si, comme le confirme l'article 6, paragraphe 3, TUE, les droits fondamentaux consacrés par la CEDH font partie du droit de l'Union en tant que principes généraux et si l'article 52, paragraphe 3, de la Charte dispose que les droits contenus dans celle-ci correspondant à des droits garantis par la CEDH ont le même sens et la même portée que ceux que leur confère ladite convention, cette dernière ne constitue pas, tant que l'Union n'y a pas adhéré, un instrument juridique formellement intégré à l'ordre juridique de l'Union (arrêts du 26 février 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, point 44 et jurisprudence citée, ainsi que du 20 mars 2018, Menci, C-524/15, EU:C:2018:197, point 22)*"

Le juge de l'Union Européenne a donné cette clé de lecture de continuité de la protection des données personnelles durant tout traitement de ces dernières, peu importe la finalité de l' "opération"[56]. Cette cohérence, dont la source européenne suffit à garantir l'efficacité, devient ainsi la clé de lecture des critères repris aux réglementations en vigueur et aux jurisprudences antérieures et utilisés à l'espèce pour les augmenter dans leur impact et leur force.[57]

B. Une renforcement des critères européens de protection

Les critères européens sont renforcés en ce qu'est bien mis en avant le fait qu'il n'est pas fait de différences entre les traitements de données, tous sont "*logés à la même enseigne*". De plus, la solidité de la matière se retrouve dans la lecture cohérente des sources textuelles et jurisprudentielles entre elles, ce qui renforce le tout.

Les critères qu'utilise le juge dans l'arrêt Schrems II n'ont rien de très novateur, mais leur interprétation apporte un regard nouveau sur la conformité de la protection des données personnelles dans le cadre de l'équilibre entre sécurité publique et vie privée. Pour reprendre et compléter une citation des Professeurs Brunessen et Sirinelli vue plus haut, le RGPD "*doit être lu, pensé, interprété comme un tout qui instaure une protection constitutionnelle européenne homogène et cohérente en dépit de la pluralité des régimes juridiques qu'il prévoit, en l'occurrence ici, de la multiplicité des fondements juridiques des transferts internationaux de données*."[58] Les critères relevés dans les arrêts Schrems I et Schrems II servent à mieux définir les obligations à respecter lorsqu'un transfert de données hors de l'Union Européenne et plus généralement lorsqu'un traitement de données à caractère

[56] Article 4.2 RGPD : «traitement», toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction;

[57] La Cour n'a pas inventé ce critère de toute pièce, déjà dans le considérant 4 de la Directive Police Justice 2016/680 évoquait ce "cadre pour la protection des données à caractère personnel solide et plus cohérent"

[58] Transfert de données vers les USA : l'arrêt Schrems II AFFAIRES | Contrat - Responsabilité IP/IT ET COMMUNICATION | Contrat – Responsabilité | Protection des données Le très attendu arrêt « Schrems II » de la Cour de justice de l'Union européenne invalide, d'une part, le bouclier de protection des données dit Privacy Shield, mais considère comme valides, d'autre part, les clauses contractuelles types de la Commission européenne. par Cécile Crichton - le 22 juillet 2020 - CJUE 16 juill. 2020, DPC c. Facebook Ireland Ltd et M. Schrems, aff. C-311/18

personnel est en cause (peu importe qu'il y ait transfert ou non). En effet, cette vision cohérente de la protection des données que veut instaurer la Cour prend sa source dans le RGPD[59] pour ensuite s'appliquer aux différents cas qui peuvent se poser, notamment aux transferts de données mais aussi à tout traitement de données qui ne rentrent pas dans les exemptions de l'article 2.2 du RGPD, et permettre d'interpréter les textes de référence en la matière. A l'aune de cet article 2.2 du RGPD, "*le présent règlement ne s'applique pas au traitement de données à caractère personnel effectué : dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union; par les États membres dans le cadre d'activités qui relèvent du champ d'application du chapitre 2 du titre V du traité sur l'Union européenne; par une personne physique dans le cadre d'une activité strictement personnelle ou domestique; par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces*." Ainsi, certes, le RGPD ne s'applique pas directement aux traitements de données qui entrent dans le champ de la sécurité publique de la Directive 2016/680 ou de la sûreté de l'Etat de l'article 31 de la Loi du 6 janvier 1978, mais la vision du juge dans l'arrêt Schrems II, fondée sur la cohérence, apporte une lecture des textes à la lumière de leur cohérence les uns avec les autres. De cette manière, sans s'appliquer directement aux types de traitements mentionnés dans l'article 2.2 du RGPD, l'idée générale de ce texte fondateur reste utile à l'interprétation des autres textes plus spécifiques, assurant ainsi une continuité de la protection des données personnels quels que soit le mode de traitement en cause. Cela rejoint l'idée du considérant 4 de la Directive Police Justice 2016/680 souhaitant un "*cadre pour la protection des données à caractère personnel solide et plus cohérent*". Le juge n'a ainsi rien "inventé" à proprement parler, il a cependant mis en lumière cet aspect harmonisé de la matière, déjà recherché par la directive e-privacy[60], et a mis des mots sur une réalité qui jusque-là n'était pas forcément prise en compte.

---

[59] Arrêts Schrems II - C-311-18 - Points 7 à 25 - énoncent tous les fondements du RGPD intéressants pour répondre aux questions préjudicielles, montrant ainsi que ce fut la majeure source d'inspiration et de fondements que le juge a utilisé pour statuer

[60] DIRECTIVE 2002/58/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) : article 1 : *La présente directive harmonise les dispositions des États membres nécessaires pour assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques, ainsi que la libre circulation de ces données et des équipements et des services de communications électroniques dans la Communauté.*

Ainsi les textes entre eux doivent être lus à l'aune d'une certaine logique dans la protection des données, ce qui empêche d'exclure entièrement le texte fondateur du RGPD ou les droits fondamentaux, quel que soit le sujet[61]. Les critères principaux pour s'assurer de la cohérence d'une protection des données conforme à la réglementation européenne se retrouvent notamment dans le RGPD et la jurisprudence de la CJUE et de la CEDH. Car si la CJUE prône son indépendance pour apporter une protection efficace aux données à caractère personnel, il n'en reste pas moins vrai que les droits fondamentaux énoncés dans la Charte des Droits Fondamentaux de l'Union Européenne doivent être lus à la lumière des mêmes droits présents dans la Conv EDH[62]. Ainsi le droit à la vie privée de l'article 8 Conv EDH reste indirectement présent dans l'arrêt Schrems II ainsi que, logiquement, la jurisprudence de la CEDH qui en découle. Et la Conv EDH ne comportant pas de droit spécifique à la protection des données personnelles, les arrêts de la Cour Européenne sur le sujet de la protection des données se réfère à l'article 8 de la Convention[63]. De plus, il ne faut pas oublier la directive 2016/680 qui n'a peut-être appliquée en l'espèce mais qui vient donner des règles supplémentaires lorsque la sécurité publique est en cause et ainsi doit être considéré dans la lignée de tout ce qui a été dit précédemment, si on reste dans cette vision continue que le juge a voulu conforter dans la matière. Tous ces textes et jugements rassemblés pour donner une vision continue d'un principe de protection des données, devenu fondamental puisqu'inscrit dans la Charte des droits fondamentaux[64], tentent d'assurer la confidentialité et la loyauté dans les traitements de données. Il faut donc que les données soient traitées en cohérence avec le RGPD dans le plus grand nombre de cas possible, en reprenant ainsi les obligations principales qui y sont édictées, notamment les exigences concernant la base légale, les droits des personnes, les durées de conservation etc. Ces critères textuels ont été affirmés déjà précédemment dans l'arrêt Schrems I de 2015[65]. Dans

[61] La cohérence de fond prônée dans l'arrêt Schrems II permet de venir à cette conclusion, en adaptant les spécificités des traitements non compris dans le champ d'application du RGPD. Pour reprendre l'exemple de la Dir. 2016/680, le droit à la portabilité n'est pas prévu par le texte contrairement au RGPD, mais c'est un détail expliqué par l'importance du maintien de la sécurité publique. Le cohérence de fond de la protection des données n'est pas entachée et l'idée générale du RGPD reste présente.

[62] Article 52§3 CDFUE : Dans la mesure où la présente Charte contient des droits correspondant à des droits garantis par la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention. Cette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue.

[63] Pour un exemple : CEDH, 17 oct. 2019, nos 1874/13 et 8567/13, Lopez Ribalda et a. c/ Espagne, Linos-Alexandre Sicilianos, prés.

[64] Article 8 Charte des droits fondamentaux : 1. Toute personne a droit à la protection des données à caractère personnel la concernant. 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.

[65] C-362/14 - Schrems - Arrêt CJUE Grande chambre 6 octobre 2015

cette décision par exemple, la cour de justice de l'Union européenne a bien mis en avant que la constitutionnalisation de la protection des données personnelles à l'article 8§3 de la Charte des Droits Fondamentaux de l'Union Européenne donne en conséquence une obligation de mettre en place une autorité indépendante pour assurer le respect de ce droit fondamental.[66] La maître de conférence Olivia Tambou commente cette affirmation en disant que "*cette indépendance est une condition essentielle pour assurer l'efficacité et la fiabilité du contrôle du respect de la protection des données personnelles par l'ensemble des acteurs qu'ils soient des entreprises ou des États*."[67] Il devient ainsi réellement clair que les arrêts Schrems ne sont pas juste des arrêts qui parlent de la compatibilité des lois de surveillance à la protection des données personnelles, mais plus généralement ce sont des arrêts qui donnent les fondamentaux en matière de traitements loyaux et de garanties autour des données personnelles, quelle que soit la situation (commerciale, fiscale, sécuritaire ou autre).

Ce sont donc les critères européens de protection des données données qui sont rappelés et renforcés. Toujours dans le même article, Olivia Tambou analyse cette position de la cour de justice comme une volonté de se placer comme une cour constitutionnelle garantissant une forte protection des données.[68] Et cette protection cohérente des données personnelles trouve sa prolongation et une de ses applications dans les transferts de données.

---

[66] C-362/14 - Schrems - Arrêt CJUE Grande chambre 6 octobre 2015 - Point 41 : La garantie d'indépendance des autorités nationales de contrôle vise à assurer l'efficacité et la fiabilité du contrôle du respect des dispositions en matière de protection des personnes physiques à l'égard du traitement des données à caractère personnel et doit être interprétée à la lumière de cet objectif. Elle a été établie en vue de renforcer la protection des personnes et des organismes qui sont concernés par les décisions de ces autorités. L'institution, dans les États membres, d'autorités de contrôle indépendantes constitue donc, ainsi que le relève le considérant 62 de la directive 95/46, un élément essentiel du respect de la protection des personnes à l'égard du traitement des données à caractère personnel (voir arrêts Commission/Allemagne, C‑518/07, EU:C:2010:125, point 25, ainsi que Commission/Hongrie C‑288/12, EU:C:2014:237, point 48 et jurisprudence citée).

[67] Propos libres autour de l'invalidation par la CJUE de la décision Safe Harbor - Source : Dalloz Actualités - 9 octobre 2015 - Olivia Tambou

[68] Propos libres autour de l'invalidation par la CJUE de la décision Safe Harbor - Source : Dalloz Actualités - 9 octobre 2015 - Olivia Tambou : "L'arrêt *Schrems* du 6 octobre 2015 constitue le troisième arrêt de Grande Chambre rendu par la CJUE en un peu plus d'un an dans le domaine de la protection des données personnelles, après les arrêts *Google Spain* et *Digital Rights Ireland*. Le point commun entre ces arrêts résulte dans la volonté de la CJUE de se poser en cour constitutionnelle, chargée de veiller au respect des droits fondamentaux inscrits dans la Charte des droits fondamentaux de l'Union européenne (UE). La CJUE garantit ainsi un niveau élevé de protection des données personnelles dans l'UE et auprès des citoyens européens."

Section 2 : Une continuité dans les transferts de données

La continuité de la protection des données personnelles dans les transferts de données se retrouve à deux niveaux : à un niveau formel tout d'abord c'est-à-dire selon le mode de transfert (A), puis à un niveau substantiel sur l'interprétation du critère de l'adéquation (B).

A. Une cohérence formelle entre les modes de transferts

Le RGPD et le document soumis par le groupe de travail de l'article 29 sur les transferts de données[69] montrent tous deux que le mode de transfert n'importe pas pour donner la mesure de la protection à apporter aux données. Quel que soit le fondement du transfert, clauses contractuelles types, décision d'adéquation, règles d'entreprises contraignantes etc. le niveau de sécurité et d'attention à apporter aux données à caractère personnel doit être le même.

Les dispositions relatives aux décisions d'adéquation, clauses contractuelles types et toute autre fondement de transfert du chapitre V du RGPD "*visent,"* selon cette décision, *"à assurer la continuité du niveau élevé de cette protection en cas de transfert de données à caractère personnel vers un pays tiers*"[70]. De cette façon, la Cour précise que malgré l'absence de décision d'adéquation, un transfert de données ne peut pas se voir doté d'une moindre protection si la base sur lequel il s'exécute se trouve être des clauses contractuelles types, des règles d'entreprises contraignante ou un code de conduite au sens de l'article 46 du RGPD.[71] En effet le but de la Cour dans l'arrêt Schrems est d'assurer la sécurité quel que soit le moyen légal utilisé pour le transfert.[72]

---

[69] Groupe de travail «Article 29» - Critères de référence pour l'adéquation - Adoptés le 28 novembre 2017 - Version révisée et adoptée le 6 février 2018

[70] CJUE 16 juillet 2020, Schrems II - Point 93 : les dispositions du chapitre V du RGPD visent à assurer la continuité du niveau élevé de cette protection en cas de transfert de données à caractère personnel vers un pays tiers, conformément à l'objectif précisé au considérant 6 de ce règlement.

[71] Idée reprise dans les recommandations du comité européen de la protection des données : Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data - Adopted on 10 November 2020

[72] Point 96 de l'arrêt : les personnes dont les données à caractère personnel sont transférées vers un pays tiers sur le fondement de clauses types de protection des données bénéficient, comme dans le cadre d'un transfert fondé sur une décision d'adéquation, d'un niveau de protection substantiellement équivalent à celui garanti au sein de l'Union.

Le groupe de travail de l'article 29 de la directive 95/46/CE a adopté un texte pour donner les critères de référence afin de traiter les demandes de décision d'adéquation[73], ce document a été actualisé pour répondre au nouvel article 45 du RGPD. Selon cet article, pour qu'un transfert de données soit autorisé hors de l'Union Européenne, l'Etat tiers doit présenter un niveau de *protection adéquat.* Le RGPD précise explicitement que ce niveau ne signifie pas que les moyens doivent être similaires[74] à ceux de l'Union Européenne mais que ce soient des moyens qui effectivement assurent à leur manière une protection essentiellement *équivalente*[75]. L'article 45 paragraphe 2 du RGPD dispose en sus qu'il est nécessaire de prendre en compte les lois de surveillance des Etats Tiers pour évaluer l'adéquation. L'arrêt Schrems II ne modifie pas ces critères, il les reprend[76], les interprète et les adapte aux transferts fondés sur des clauses contractuelles types puisque la décision d'adéquation est déniée en l'espèce. Le point le plus important, peut-être, tient dans la notion *d'équivalence* qui revient une vingtaine de fois dans l'affaire[77]. Cette équivalence est analysée à partir d'un faisceau d'indices qui peut être repris aux critères d'adéquation trouvés par le groupe de travail de l'article 29 précité. En effet dans un chapitre 3, le groupe de travail énumère les " *Principes généraux en matière de protection des données visant à garantir que le niveau de protection dans un pays tiers, un territoire ou un ou plusieurs secteurs déterminé au sein de ce pays tiers ou d'une organisation internationale est substantiellement équivalent à celui garanti par la législation européenne"*. Or dans l'arrêt Schrems II, il est bien question de s'assurer que les données bénéficient d'une protection adéquate et "substantiellement équivalente[78]" pour que des clauses contractuelles types fondent un transfert à la place d'une

---

[73] Groupe de travail «Article 29» - Critères de référence pour l'adéquation - Adoptés le 28 novembre 2017 - Version révisée et adoptée le 6 février 2018 - précité

[74] Point 94 de l'arrêt Schrems II : "*À cet égard, sans exiger que le pays tiers concerné garantisse un niveau de protection identique à celui garanti dans l'ordre juridique de l'Union….*"

[75] Considérant 104 du RGPD : "*Lors de l'adoption, à l'égard d'un territoire ou d'un secteur déterminé dans un pays tiers, d'une décision d'adéquation, il y a lieu de tenir compte de critères clairs et objectifs, tels que les activités de traitement spécifiques et le champ d'application des normes juridiques applicables et de la législation en vigueur dans le pays tiers. Le pays tiers devrait offrir des garanties pour assurer un niveau adéquat de protection essentiellement équivalent à celui qui est garanti dans l'Union, en particulier quand les données à caractère personnel sont traitées dans un ou plusieurs secteurs spécifiques"*

[76] Point 94 de l'arrêt

[77] Points 64 / 65 / 94 / 96 / 97 / 107 / 133 / 163/ 178 / 180 / 181 / 185 / 190 / 191 / 197 etc.

[78] Point 105 de l'arrêt : *"Partant, il y a lieu de répondre aux deuxième, troisième et sixième questions que l'article 46, paragraphe 1, et l'article 46, paragraphe 2, sous c), du RGPD doivent être interprétés en ce sens que les garanties appropriées, les droits opposables et les voies de droit effectives requis par ces dispositions doivent assurer que les droits des personnes dont les données à caractère personnel sont transférées vers un pays tiers sur le fondement de clauses types de protection des données bénéficient d'un niveau de protection substantiellement équivalent à celui garanti au sein de l'Union par ce règlement, lu à la lumière de la Charte. À cet effet, l'évaluation du niveau de protection assuré dans le contexte d'un tel transfert doit, notamment, prendre en considération tant les stipulations contractuelles convenues entre le responsable du traitement ou son*

décision d'adéquation. Finalement le même niveau de protection des données est demandé, quelle que soit la situation, que le transfert soit fondé sur des clauses contractuelles ou sur une adéquation[79]. Cette lecture se retrouve dans l'arrêt Schrems II et prouve bien la volonté qu'a le juge a garantir la cohérence de la protection des données personnelles, quel que soit le fondement du transfert de données.

Après ce critère formel de cohérence de la protection dans les transferts de données, il faut analyser un autre critère substantiel de continuité de la notion d'adéquation lors de ces derniers.

B. Une continuité substantielle de la notion d'adéquation

La continuité substantielle de la notion d'adéquation se retrouve dans les arrêts Schrems I et II dans les critères utilisés pour fonder un transfert sur une décision d'adéquation ou sur des clauses contractuelles types.

L'article 45 du RGPD et les critères du groupe de travail de l'article 29 peuvent être utilisés pour vérifier si un transfert de données fondé sur des clauses contractuelles types est valable. L'article 45 paragraphe 2 donne le principe de la prise en compte, notamment, des lois de surveillance des Etats Tiers pour évaluer l'adéquation, ce qui doit impérativement être repris pour assurer la protection des données lors de la mise en place de clauses contractuelles type, quitte à renforcer les mesures de base mise en place par de telles clauses[80]. Il faut tenir

---

sous-traitant établis dans l'Union et le destinataire du transfert établi dans le pays tiers concerné que, en ce qui concerne un éventuel accès des autorités publiques de ce pays tiers aux données à caractère personnel ainsi transférées, les éléments pertinents du système juridique de celui-ci, notamment ceux énoncés à l'article 45, paragraphe 2, dudit règlement."

[79] Conclusions de l'avocat général - M. HENRIK SAUGMANDSGAARD ØE - présentées le 19 décembre 2019 (1) Affaire C-311/18 - **Point 112 et 113.** 112. Cette juridiction souligne que, dans l'arrêt Schrems, la Cour a interprété l'article 25, paragraphe 6, de la directive 95/46 (dont le contenu est essentiellement repris à l'article 45, paragraphe 3, du RGPD), en ce qu'il prévoyait que la Commission ne peut adopter une décision d'adéquation qu'après s'être assurée que le pays tiers visé garantit un niveau de protection adéquat, comme supposant que celle-ci établisse que ce pays assure un niveau de protection des libertés et droits fondamentaux substantiellement équivalent à celui garanti au sein de l'Union en vertu de cette directive, lue à la lumière de la Charte (42). 113. Dans ce contexte, la première partie de la sixième question préjudicielle invite la Cour à déterminer si l'application de « clauses contractuelles types » adoptées par la Commission en application de l'article 26, paragraphe 4, de la directive 95/46 – correspondant aux « clauses types de protection » désormais mentionnées à l'article 46, paragraphe 2, sous c), du RGPD – doit permettre d'atteindre un niveau de protection correspondant au même standard d'« équivalence substantielle ».

[80] Point 133 de l'arrêt *: "Il apparaît ainsi que les clauses types de protection des données adoptées par la Commission au titre de l'article 46, paragraphe 2, sous c), du même règlement visent uniquement à fournir aux*

compte ainsi de *"l'état de droit, le respect des droits de l'homme et des libertés fondamentales, la législation pertinente, tant générale que sectorielle, y compris en ce qui concerne la sécurité publique, la défense, la sécurité nationale et le droit pénal ainsi que l'accès des autorités publiques aux données à caractère personnel"..."la jurisprudence, ainsi que les droits effectifs et opposables dont bénéficient les personnes concernées et les recours administratifs et judiciaires que peuvent effectivement introduire les personnes concernées dont les données à caractère personnel sont transférées" et "l'existence et le fonctionnement effectif d'une ou de plusieurs autorités de contrôle indépendantes dans le pays tiers, ou auxquelles une organisation internationale est soumise, chargées d'assurer le respect des règles en matière de protection des données et de les faire appliquer"*. Cela induit qu'il est nécessaire de vérifier que quatre conditions sont réunies pour considérer qu'il existe une protection essentiellement équivalente dans le cadre des lois de surveillance et de leur équilibre avec le principe de protection de la vie privée[81] et donc qu'il y a une proportionnalité de l'ingérence des autorités publiques dans les données personnelles[82] :

- si le traitement repose sur des règles claires, précises et accessibles ;
- s'il y a des démonstrations de nécessité et de proportionnalité au regard des objectifs légitimes poursuivis ;
- si le traitement fait l'objet d'un contrôle indépendant ;
- et si les particuliers disposent de voies de recours effectives.

Plus précisément, il faut que le traitement opéré sur les données personnelles dans l'Etat tiers soit loyal, licite et visant des finalités légitimes. Le groupe de travail de l'article 29 donne d'autres critères fondamentaux qu'on retrouve dans le RGPD pour qualifier l'adéquation, il y a par exemple la vérification de la présence d'un principe de minimisation des données, de règles entourant la conservation des données, de proportionnalité, de sécurité, de

---

responsables du traitement ou à leurs sous-traitants établis dans l'Union des garanties contractuelles s'appliquant de manière uniforme dans tous les pays tiers et, dès lors, indépendamment du niveau de protection garanti dans chacun d'entre eux. Dans la mesure où ces clauses types de protection des données ne peuvent, eu égard à leur nature, fournir des garanties allant au-delà d'une obligation contractuelle de veiller à ce que le niveau de protection requis par le droit de l'Union soit respecté, elles peuvent nécessiter, en fonction de la situation prévalant dans tel ou tel pays tiers, l'adoption de mesures supplémentaires par le responsable du traitement afin d'assurer le respect de ce niveau de protection."

[81] Groupe de travail «Article 29» - Critères de référence pour l'adéquation - Adoptés le 28 novembre 2017 - Version révisée et adoptée le 6 février 2018 - Chapitre 4 : Garanties essentielles dans les pays tiers en matière d'application des lois et d'accès pour raison de sécurité nationale afin de limiter les ingérences dans les droits fondamentaux

[82] Cf supra note 44 : "*La base légale qui permet l'ingérence dans ces droits doit donc définir elle-même la portée de la limitation de l'exercice du droit et prévoir des règles claires et précises régissant la portée et l'application de la mesure".*

confidentialité, de transparence, d'accès, de rectification, d'effacement et il vérifie les recours et les garanties offertes aux citoyens[83].

Tout cela vaut certes pour analyser la conformité de la protection des données personnelles dans le cadre d'une décision d'adéquation mais aussi pour fonder un transfert sur des clauses contractuelles types. Ainsi l'évaluation du caractère "*adéquat*" et "*substantiellement équivalent*" du niveau de protection réside sur des critères reprenant des règles de fond considérées comme essentielles et sur une étude de l'efficacité du dispositif implanté pour garantir l'applicabilité de ces règles, même face à des lois de surveillance. Pour cela, l'arrêt Schrems II met en avant son critère de cohérence et demande à ce que les transferts fondés sur une autre base qu'une décision d'adéquation, par exemple sur des clauses contractuelles types, s'exécutent en s'adaptant à l'Etat tiers pour assurer une protection efficace des données, et cela en prenant en compte les mêmes critères que la commission lorsqu'elle analyse l'adéquation de la protection d'un Etat avec les règles européennes.[84] De là, elle oblige à prendre des mesures renforcées ("*garanties appropriées*") lorsque les clauses contractuelles types ne suffisent pas à elles seules pour assurer cette protection en se fondant sur les considérants du RGPD[85]. Et enfin pour que la cohérence dans

---

[83] Groupe de travail «Article 29» - Critères de référence pour l'adéquation - Adoptés le 28 novembre 2017 - Version révisée et adoptée le 6 février 2018 - Chapitre 3: Principes généraux en matière de protection des données visant à garantir que le niveau de protection dans un pays tiers, un territoire ou un ou plusieurs secteurs déterminés au sein de ce pays tiers ou d'une organisation internationale est substantiellement équivalent à celui garanti par la législation européenne - Le système d'un pays tiers ou d'une organisation internationale doit comporter les principes et mécanismes fondamentaux suivants touchant au contenu des règles sur la protection des données et aux exigences en matière de procédure/d'application

[84] Point 108 de l'arrêt : En l'absence de décision d'adéquation, le responsable du traitement ou le sous-traitant devrait prendre des mesures pour compenser l'insuffisance de la protection des données dans le pays tiers par des garanties appropriées en faveur de la personne concernée. Ces garanties peuvent consister à recourir à des règles d'entreprise contraignantes, des clauses types de protection des données adoptées par la Commission, des clauses types de protection des données adoptées par une autorité de contrôle ou des clauses contractuelles autorisées par une autorité de contrôle. Ces garanties devraient assurer le respect des exigences en matière de protection des données et des droits des personnes concernées d'une manière appropriée au traitement au sein de l'Union, y compris l'existence de droits opposables de la personne concernée et de voies de droit effectives, ce qui comprend le droit d'engager un recours administratif ou juridictionnel effectif et d'introduire une action en réparation, dans l'Union ou dans un pays tiers. Ces garanties devraient porter, en particulier, sur le respect des principes généraux concernant le traitement des données à caractère personnel et des principes de protection des données dès la conception et de protection des données par défaut. [...]

[85] Points 131 et 132 de l'arrêt : 131. À cet égard, il y a lieu de rappeler que, aux termes de l'article 46, paragraphe 1, de ce règlement, en l'absence de décision d'adéquation de la Commission, il incombe au responsable du traitement ou au sous-traitant établis dans l'Union de prévoir, notamment, des garanties appropriées. Les considérants 108 et 114 dudit règlement confirment que, lorsque la Commission ne s'est pas prononcée sur le caractère adéquat du niveau de protection des données dans un pays tiers, le responsable du traitement ou, le cas échéant, son sous-traitant « devrait prendre des mesures pour compenser l'insuffisance de la protection des données dans le pays tiers par des garanties appropriées en faveur de la personne concernée » et que « [c]es garanties devraient assurer le respect des exigences en matière de protection des données et des droits des personnes concernées d'une manière appropriée au traitement au sein de l'Union, y compris l'existence de droits opposables de la personne concernée et de voies de droit effectives [...] dans l'Union ou

la protection des données soit véritablement efficace, la Cour prône un pouvoir important des autorités de contrôle protégeant les données transférées, notamment via des clauses contractuelles types, et assurant la conformité de leur sécurité avec les critères demandés.[86] Et pour que ces autorités soient véritablement efficaces dans leur protection il est nécessaire qu'elles soient indépendantes, comme le préconisait déjà le juge dans l'arrêt Schrems I de 2015.[87]

---

dans un pays tiers ». 132. Dès lors que, comme il ressort du point 125 du présent arrêt, il est inhérent au caractère contractuel des clauses types de protection des données que celles-ci ne sauraient lier les autorités publiques des pays tiers, mais que l'article 44, l'article 46, paragraphe 1, et l'article 46, paragraphe 2, sous c), du RGPD, interprétés à la lumière des articles 7, 8 et 47 de la Charte, exigent que le niveau de protection des personnes physiques garanti par ce règlement ne soit pas compromis, il peut s'avérer nécessaire de compléter les garanties que contiennent ces clauses types de protection des données. À cet égard, le considérant 109 dudit règlement énonce que « [l]a possibilité qu'ont les responsables du traitement [...] de recourir à des clauses types de protection des données adoptées par la Commission [...] ne devrait pas les empêcher [...] d'y ajouter d'autres clauses ou des garanties supplémentaires » et précise, en particulier, que ceux-ci « devraient être encouragés à fournir des garanties supplémentaires [...] qui viendraient compléter les clauses types de protection [des données] ».

[86] Points 11 à 115 de l'arrêt - Point 115 : En tout état de cause, le pouvoir d'exécution que l'article 46, paragraphe 2, sous c), du RGPD reconnaît à la Commission aux fins d'adopter des clauses types de protection des données ne lui confère pas la compétence de restreindre les pouvoirs dont disposent les autorités de contrôle au titre de l'article 58, paragraphe 2, de ce règlement (voir par analogie, s'agissant de l'article 25, paragraphe 6, et de l'article 28 de la directive 95/46, arrêt du 6 octobre 2015, Schrems, C‑362/14, EU:C:2015:650, points 102 et 103). Au demeurant, le considérant 5 de la décision d'exécution 2016/2297 confirme que la décision CPT « n'empêche nullement une [autorité de contrôle] d'exercer ses pouvoirs de contrôle des flux de données, notamment le pouvoir de suspendre ou d'interdire un transfert de données à caractère personnel, lorsqu'elle constate que ce transfert est effectué en violation de la législation de l'Union européenne ou de l'État membre en matière de protection des données ».

[87] Propos libres autour de l'invalidation par la CJUE de la décision Safe Harbor - Source : Dalloz actualités - Olivia Tambou - 9 octobre 2015 : "La CJUE en déduit trois conséquences. Premièrement, elle consacre le droit pour toute personne de pouvoir saisir une autorité nationale de protection des données, si elle s'estime lésée dans ses droits fondamentaux du fait d'un transfert de ses données personnelles vers un pays tiers. Cela se traduit par la compétence des autorités nationales de protection pour examiner ce type de plainte, même en présence d'une décision de protection adéquate de la Commission. Deuxièmement, cette indépendance institutionnelle de la Commission s'accompagne également d'une indépendance procédurale. En effet, la CJUE remet en cause la possibilité pour la Commission européenne de limiter les hypothèses dans lesquelles les autorités nationales de protection des données pourraient suspendre les flux de données vers une organisation adhérant au Safe Harbor. Elle invalide ainsi l'article 3 de la décision Safe Harbor en tant que « règlementation spécifique », excluant la possibilité pour les autorités nationales de protection des données de prendre des mesures visant à s'assurer qu'aucun transfert de données personnelles n'ait lieu vers un pays n'ayant pas un niveau de protection adéquat. La CJUE rappelle également qu'en cas de doutes sérieux de la part de l'autorité nationale sur le caractère adéquat de la protection constatée dans une décision de la Commission, elle doit disposer de la possibilité d'un recours devant les juridictions nationales qui pourront, le cas échéant, interroger la CJUE à titre préjudiciel. Troisièmement, la mise en exergue des autorités nationales de protection des données dans la conception européenne interroge implicitement sur sa compatibilité avec le système américain. La CJUE ne va pas jusqu'au bout de cette logique en examinant le statut de la Federal Trade Commission (FTC). En revanche, l'avocat général rappelle que « la FTC ne joue pas un rôle comparable à celui des autorités nationales de contrôle prévues à l'article 28 de la directive 95/46 » (point 205). Il considère alors que la décision Safe Harbor aurait dû être accompagnée par « la mise en place d'un mécanisme de contrôle assuré par une autorité administrative indépendante spécialisée en matière de protection des données à caractère personnel » (pt 209)."

La cohérence des textes rejoint la cohérence dans le pouvoir de les faire respecter. Ainsi non seulement tous les textes prennent sens les uns avec les autres[88] (les articles 47, 52, 7 et 8 de la Charte des droits fondamentaux ; 6 et 8 de la Convention européenne des droits de l'homme et le RGPD) pour assurer une protection adéquate des données au sein du territoire et lors des transferts, mais aussi les moyens importants donnés aux autorités de contrôle restent dans la continuité de cette cohérence. L'idée qui règne dans l'arrêt Schrems II, dans la lignée de l'arrêt Schrems I, est celle de la cohérence dans la protection des données et cela entraîne un renforcement de cette dernière à tous les plans, sur le territoire européen et dans les transferts, en théorie. Le but étant de faire la différence entre ce qui est fondamental et ce qui est spécifique à chaque culture, et la cohérence se retrouvant dans l'aspect fondamental de la protection[89]. Cependant, en pratique, la cohérence de la protection des données en présence de lois de surveillance est souvent plus compliquée à trouver.

[88] Dalloz IP/IT - Schrems II : on prend les mêmes et on recommence – Brunessen Bertrand – Jean Sirinelli – Dalloz IP/IT 2020 - Page 640 - n°11 du 23/11/2020 : "*La détermination du niveau de protection adéquat passe aussi par l'existence d'un droit au juge. L'article 47 de la Charte participe aussi du niveau européen de protection des données en exigeant un recours effectif devant un tribunal indépendant et impartial. C'est là une exigence élémentaire de l'État de droit qui est au cœur de la jurisprudence de la Cour de justice depuis toujours (CJCE 15 mai 1986, aff. C-222/84, Johnston).*"

[89] SCHWARTZ M. (P), PEIFER (K.N), « Transatlantic Data Privacy Law », The George Town Law Journal, volume 106, 2017, pp. 115 à 179.

Partie 2 : Une antinomie persistante entre surveillance et protection

Les lois de surveillance (notion de sécurité) ne sont pas faciles à concilier avec la protection des données personnelles (liberté et vie privée), au niveau européen et interne, (section 1) et encore au niveau des transferts de données et de l'adéquation de la protection à respecter (section 2).

Section 1 : Des lois de surveillance européennes contestées

Il est intéressant de noter en premier lieu que l'arrêt Schrems II reste dans la continuité de l'ingérence des juges européens et de l'Union européenne pour préserver l'intégrité de la protection des données dans les politiques sécuritaires de renseignement. Ces derniers apportent en conséquence de nombreux garde-fous aux lois de surveillance (A) qui, s'il ne sont pas respectés, entraînent des sanctions des juges ou au moins des recours (B).

A. La cohérence des garde-fous entre les juges européens

L'arrêt Schrems II s'ajoute aux anciens arrêts de la CJUE et de la CEDH pour renforcer la position protectrice des données malgré la visée sécuritaire des lois de surveillance. Ainsi la jurisprudence de la CJUE et celle de la CEDH ont tenté de donner des garde-fous à la latitude des Etats à définir leurs lois de surveillance.

En théorie, la continuité de la protection prônée par la cour de Justice dans l'arrêt Schrems II renforce cette dernière dans l'ordre européen des Etats et de leurs lois de surveillance. Certainement que le critère de la donnée traitée à titre commercial et qui fait ensuite l'objet d'un traitement aux fins de sécurisation de l'Etat et de surveillance de celui-ci peut être repris ici[90]. Cela permettrait de ne pas rendre inapplicable le RGPD au traitement de données effectué par des organismes de surveillance puisque la continuité de la protection de

[90] Cf infra partie 1 - 1 - A

la donnée en question permet de passer outre l'exemption de l'article 2.2 du RGPD[91] selon l'arrêt Schrems II. [92] De même, a priori, on aurait pu imaginer que l'Union européenne n'étant pas compétente en matière de sécurité nationale, les arrêts de la cour de justice ne s'appliquent pas aux techniques de renseignement et de surveillance des articles du code de la sécurité intérieure sur la lutte pour les" intérêts fondamentaux de la Nation."[93] La cour de justice est déjà venue clarifier ce point dans une affaire du 6 octobre 2020[94]. Tout d'abord elle a rappelé dans les points 135 et 136 que l'article 4 du TUE donne une compétence exclusive aux Etats en matière de sécurité nationale[95]. Dans ce cadre où les menaces contre la stabilité de l'Etat sont plus importantes que dans la lutte contre la criminalité même grave, il est possible de prendre des "*mesures comportant des ingérences dans les droits fondamentaux plus graves que celles que pourraient justifier ces autres objectifs"* (point 136). Cependant les points 137, 138 et 139 limitent ce pouvoir pourtant exclusif des Etats à la lumière des articles 7, 8, 11 et 52 de la Charte des droits fondamentaux.[96] Ainsi, même lorsque la sécurité

---

[91] Le présent règlement ne s'applique pas au traitement de données à caractère personnel effectué : a) dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union; b) par les États membres dans le cadre d'activités qui relèvent du champ d'application du chapitre 2 du titre V du traité sur l'Union européenne; c) par une personne physique dans le cadre d'une activité strictement personnelle ou domestique; d) par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces.

[92] Arrêt Schrems II -C-311/18 - Points 80 à 89

[93] CE 26 juill. 2018, req. n° 394922- Résumé : "*Dès lors, ces dispositions ne sauraient être regardées comme mettant en oeuvre le droit de l'Union européenne et, par suite, les moyens tirés de la méconnaissance de la directive du 12 juillet 2002 interprétée à la lumière de la Charte des droits fondamentaux de l'Union européenne ne peuvent être utilement invoqués à leur encontre.*"

[94] Arrêt de la Cour (grande chambre) du 6 octobre 2020 - La Quadrature du Net e.a. contre Premier ministre e.a. - Affaires jointes C-511/18, C-512/18 et C-520/18

[95] Arrêt de la Cour (grande chambre) du 6 octobre 2020 - La Quadrature du Net e.a. contre Premier ministre e.a. - Affaires jointes C-511/18, C-512/18 et C-520/18 : points 135 et 136 . 135. À cet égard, il convient de relever, d'emblée, que l'article 4, paragraphe 2, TUE énonce que la sécurité nationale reste de la seule responsabilité de chaque État membre. Cette responsabilité correspond à l'intérêt primordial de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société et inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme.136. Or, l'importance de l'objectif de sauvegarde de la sécurité nationale, lu à l'aune de l'article 4, paragraphe 2, TUE, dépasse celle des autres objectifs visés à l'article 15, paragraphe 1, de la directive 2002/58, notamment des objectifs de lutte contre la criminalité en général, même grave, ainsi que de sauvegarde de la sécurité publique. En effet, des menaces telles que celles visées au point précédent se distinguent, par leur nature et leur particulière gravité, du risque général de survenance de tensions ou de troubles, même graves, à la sécurité publique. Sous réserve du respect des autres exigences prévues à l'article 52, paragraphe 1, de la Charte, l'objectif de sauvegarde de la sécurité nationale est dès lors susceptible de justifier des mesures comportant des ingérences dans les droits fondamentaux plus graves que celles que pourraient justifier ces autres objectifs.

[96] Arrêt de la Cour (grande chambre) du 6 octobre 2020 - La Quadrature du Net e.a. contre Premier ministre e.a. - Affaires jointes C-511/18, C-512/18 et C-520/18 :

137. "*Ainsi, dans des situations telles que celles décrites aux points 135 et 136 du présent arrêt, l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne s'oppose pas, en principe, à une mesure législative qui autorise les autorités compétentes à enjoindre aux fournisseurs de services de communications électroniques de procéder à la*

nationale, la sauvegarde des intérêts fondamentaux, sont en jeu, les Etats doivent limiter l'injonction de conservation des données au strict nécessaire, qu'un temps limité soit prévu, que des garanties contre les abus soient offertes et que des contrôles par une autorité compétente soient effectués.[97] Le but étant d'empêcher que la conservation généralisée des données devienne la règle. Sur cette question la CJUE avait déjà eu à se positionner dans deux affaires : l'arrêt du 8 avril 2014, Digital Rights Ireland[98] ; l'arrêt du 21 décembre 2016, Tele2 Sverige[99]. Certains parlent alors d'une "objectivisation de la notion d'intérêt public"[100], car l'objectivité permet la cohérence : l'objectivité dans la protection des données permet donc la cohérence dans cette protection.

La CEDH donne aussi son interprétation de l'article 8 de la Convention pour limiter l'ingérence de l'Etat dans la vie privée des personnes concernées, cette interprétation faisant indirectement corps avec l'article 7 de la Charte des Droits Fondamentaux de l'Union Européenne du fait de l'interprétation conforme de l'article 52§3 de la Charte. Ainsi la Cour a pu préciser dans le point 227 de son arrêt du 4 décembre 2015, Roman Zakharov c. Russie

---

conservation des données relatives au trafic et des données de localisation de l'ensemble des utilisateurs des moyens de communications électroniques pendant une période limitée, dès lors qu'il existe des circonstances suffisamment concrètes permettant de considérer que l'État membre concerné fait face à une menace grave telle que celle visée aux points 135 et 136 du présent arrêt pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible. Même si une telle mesure vise, de manière indifférenciée, tous les utilisateurs de moyens de communications électroniques sans que ceux-ci paraissent, de prime abord, présenter de rapport, au sens de la jurisprudence visée au point 133 du présent arrêt, avec une menace pour la sécurité nationale de cet État membre, il y a lieu néanmoins de considérer que l'existence d'une telle menace est de nature, par elle-même, à établir ce rapport."

138. *"L'injonction prévoyant la conservation préventive des données de l'ensemble des utilisateurs des moyens de communications électroniques doit, néanmoins, être temporellement limitée au strict nécessaire. S'il ne peut être exclu que l'injonction faite aux fournisseurs de services de communications électroniques de procéder à la conservation des données puisse, en raison de la persistance d'une telle menace, être renouvelée, la durée de chaque injonction ne saurait dépasser un laps de temps prévisible. De surcroît, une telle conservation des données doit être sujette à des limitations et encadrée par des garanties strictes permettant de protéger efficacement les données à caractère personnel des personnes concernées contre les risques d'abus. Ainsi, cette conservation ne saurait présenter un caractère systématique.*"

139. "*Eu égard à la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte résultant d'une telle mesure de conservation généralisée et indifférenciée des données, il importe d'assurer que le recours à celle-ci soit effectivement limité aux situations dans lesquelles il existe une menace grave pour la sécurité nationale, telles que celles visées aux points 135 et 136 du présent arrêt. À cet effet, il est essentiel qu'une décision faisant injonction aux fournisseurs de services de communications électroniques de procéder à une telle conservation des données puisse faire l'objet d'un contrôle effectif soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties devant être prévues*."

[97] BONNEVILLE Philippe ; GÄNSER Christian ; MARKARIAN Sophie ; ILJIC Anne - Chronique de jurisprudence de la CJUE - in AJDA 2021. p. 387

[98] CJUE 8 avril 2014 C-293/12 - Digital Rights Ireland et Seitlinger e.a.

[99] CJUE 21 décembre 2016 C-203/15 - Tele2 Sverige

[100] Privacy International & La Quadrature du Net: the latest on data retention in the name of national and public security – Part 1 BY PLIXAVRA VOGIATZOGLOU AND JENNY BERGHOLM - 15 OCTOBER 2020

qu'une ingérence dans la vie privée ne peut se justifier que si certaines conditions sont remplies : que cette ingérence est prévue par la loi, qu'elle vise un but légitime ("la sécurité nationale, la sûreté publique, le bien-être économique du pays, la défense de l'ordre et à la prévention des infractions pénales, la protection de la santé ou de la morale, ou la protection des droits et libertés d'autrui"[101]) et qu'elle soit nécessaire pour atteindre ces buts. Le critère étant celui de la nécessité "dans une société démocratique"[102]. La durée de l'ingérence est aussi mise en cause par cet arrêt. La note d'information de la cour sur cet arrêt précise bien que les lois de surveillance internes doivent comporter, "*au sujet de la durée et de la prorogation d'une mesure d'interception, des règles claires qui offrent des garde-fous adéquats contre les abus*" et que a contrario *"les dispositions pertinentes sur la levée de mesures de surveillance ne fournissent pas des garanties suffisantes contre les ingérences arbitraires."*[103]

Ainsi la CJUE et la CEDH posent des limites à ce qu'il est possible de faire dans le cadre des lois de surveillance, afin de garder un équilibre entre la sécurité et la protection des données. Cependant cela n'est pas toujours accepté par les Etats qui se voient contraints dans leur politique alors même qu'il s'agit d'un sujet qui devrait relever uniquement de la compétence nationale.[104]

---

[101] Article 8 §2 Conv EDH

[102] CEDH, Roman Zakharov c. Russie [GC], n° 47143/06, 4 décembre 2015, point 227

[103] Note d'information sur la jurisprudence de la Cour 191- Décembre 2015 - Roman Zakharov c. Russie [GC] - 47143/06 - page 3 - iii. Durée des mesures de surveillance secrète

[104] Conservation des données : le gouvernement demande au Conseil d'État d'ignorer la justice européenne - Source : Nextinpact - Marc Rees - 3 mars 2021 : *"Selon nos informations, le gouvernement a invité le Conseil d'État à suivre une voie exceptionnelle : se draper derrière l'étendard de la souveraineté nationale et même de l'identité constitutionnelle de la France pour ne pas appliquer les mesures imposées par la CJUE. Il considère que ces juges ont fait une bien mauvaise application du traité de l'UE en allant au-delà de leurs compétences. Pourquoi ? Toujours selon nos sources gouvernementales, l'exécutif estime que cette jurisprudence vient priver d'effectivité plusieurs principes constitutionnels français, dont le principe de sauvegarde des intérêts fondamentaux de la nation, l'objectif de prévention, de recherches des auteurs d'infraction pénale, et l'objectif de lutte contre le terrorisme. Interdire la conservation généralisée des données de connexion, sauf dans quelques cas trop spécifiques, priverait finalement la France des moyens d'actions nécessaires pour assurer la mise en œuvre de ces principes fondateurs. Un véritable « bras d'honneur » adressé à la CJUE qui ne surprend pas vraiment. Au même moment, le gouvernement milite aussi pour colmater cette brèche dans le futur, au travers du projet de règlement ePrivacy, comme l'a souligné le professeur Theodore Christakis le long d'un « thread » sur Twitter. De même, à l'Assemblée nationale, le député Guillaume Larrivé a déjà dénoncé le « hold-up » des décisions de la CJUE en matière de conservation des données de connexion. Dans son rapport sur les cinq ans de la loi Renseignement, l'élu LR estime qu'« on n'aurait sans doute d'autre solution que de considérer que la primauté du droit européen cesse quand on se trouve au cœur du cœur de la souveraineté nationale et de notre droit constitutionnel ».*

B. Des sanctions et invalidations régulièrement ordonnées

Les limites sont édictées dans les arrêts de la CEDH ou de la CJUE, dans les textes des lois de surveillance qui rappellent les principes[105] et soutiennent que toute ingérence doit être prévue et limitée par la loi. Cependant, les rappels et les garde-fous n'empêchent pas les Etats européens d'être condamnés ou de risquer de l'être.

Les pays européens ont déjà été sanctionnés sur leurs manières d'effectuer le renseignement afin de mener à bien leur politique de surveillance. Les arrêts précités en sont la preuve. En effet, après l'affaire Télé2 Sverige qui énonce l'interdiction d'« *une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique* »[106], le conseil d'Etat a posé une question préjudicielle à la Cour de Justice[107] afin de remettre en cause cette solution.[108] Selon lui, "*dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, tenant en particulier au risque terroriste, ces techniques présentent ainsi une utilité opérationnelle sans équivalent.*[109]" Les articles L851-1 à 3 du code de la sécurité intérieure sur la collecte des données de connexion uniquement techniques ont été citées pour cela. La cour de justice a répondu dans l'arrêt du 6 octobre 2020, La Quadrature du Net, en affirmant

---

[105] Par exemple : L 801-1 code de la sécurité intérieure : Le respect de la vie privée, dans toutes ses composantes, notamment le secret des correspondances, la protection des données à caractère personnel et l'inviolabilité du domicile, est garanti par la loi. L'autorité publique ne peut y porter atteinte que dans les seuls cas de nécessité d'intérêt public prévus par la loi, dans les limites fixées par celle-ci et dans le respect du principe de proportionnalité.

[106] CJUE 21 décembre 2016 - affaires jointes C-203/15 et C-698/15 : Décision de la cour 1) L'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique.

[107] CE 26 juill. 2018, req. n° 394922 précité

[108] Techniques de renseignement : quand le Conseil d'État invite la CJUE à revoir sa jurisprudence - Par Marie-Christine de Montecler - Source Dalloz Actualités - Le 7 septembre 2018 - *"Êtes-vous vraiment sûrs que, dans le contexte de menace terroriste, il faut interdire la conservation généralisée des données de connexion ? Telle est la question que le Conseil d'État a renvoyée en juillet à la CJUE et dont la formulation invite assez clairement les juges de Luxembourg à revenir sur leur jurisprudence."*

[109] CE 26 juill. 2018, req. n° 394922 - point 27

sa compétence et en interdisant une nouvelle fois la conservation généralisée des données[110], sauf s'il existe une *"menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible*" (Premier paragraphe de la décision CJUE 6 octobre 2020 précitée) ou que ces données soient délimitées objectivement etc. L'avocat Général M. Manuel Campos Sanchez-Bordona précisant que selon lui la lutte contre le terrorisme « *ne doit pas être envisagée uniquement au regard de son efficacité* » car « *si les pouvoirs publics étaient dotés d'instruments démesurés aux fins de la poursuite de l'infraction, leur permettant d'ignorer ou de dénaturer les droits fondamentaux, rien ne pourrait faire obstacle à ce que leur action incontrôlée et entièrement libre s'exerce en fin de compte au détriment de la liberté de tous* » (pt 131)[111].Ainsi elle condamne la France à revoir ses dispositions du code de la sécurité intérieure, notamment les articles L 851-1 à 3. La France n'est pas la seule à avoir été condamnée, le Royaume Uni l'a aussi été en 2018[112] par la CEDH. Celle-ci confirme que "la décision de recourir à un régime d'interception massive de communications (tel que prévu par la section 8[4] du Regulation of Investigatory Powers Act 2000) relève de la marge nationale d'appréciation (§ 387)."[113] Cependant cela n'empêche pas la cour d'être compétente pour vérifier que la mise en œuvre de cette surveillance reste dans la limite de l'article 8 de la Convention européenne des droits de l'Homme.[114] Or dans cet arrêt la cour a considéré là aussi que la loi relative aux renseignements au Royaume-Uni ne limite pas assez les données collectées aux données résultant de "*crimes sérieux*" et qu'il n'était pas prévu de contrôle

---

[110] CJUE 6 octobre 2020 - aff. jointes C 511/18, C512/18 et C520/18 - Décision : 4) *"Une juridiction nationale ne peut faire application d'une disposition de son droit national qui l'habilite à limiter dans le temps les effets d'une déclaration d'illégalité lui incombant, en vertu de ce droit, à l'égard d'une législation nationale imposant aux fournisseurs de services de communications électroniques, en vue, notamment, de la sauvegarde de la sécurité nationale et de la lutte contre la criminalité, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec l'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux. Cet article 15, paragraphe 1, interprété à la lumière du principe d'effectivité, impose au juge pénal national d'écarter des informations et des éléments de preuve qui ont été obtenus par une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec le droit de l'Union, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité, si ces personnes ne sont pas en mesure de commenter efficacement ces informations et ces éléments de preuve, provenant d'un domaine échappant à la connaissance des juges et qui sont susceptibles d'influencer de manière prépondérante l'appréciation des faits".*

[111] DANIS-FATÔME Anne - *La protection des données personnelles résiste à la surveillance générale qu'imposerait la lutte contre le terrorisme* - in Communication Commerce électronique n° 4, Avril 2020, comm. 36

[112] CEDH 13 sept. 2018, Big Brother Watch et a. c. Royaume-Uni, nos 58170/13, 62322/14 et 24960/15

[113] Surveillance de sécurité : le Royaume-Uni condamné pour son système d'interception et d'obtention de données - Source Dalloz actualités - Sabrina Lavric - 4 octobre 2018

[114] Surveillance de sécurité : le Royaume-Uni condamné pour son système d'interception et d'obtention de données - Source Dalloz actualités - Sabrina Lavric - 4 octobre 2018 : "la violation de l'article 8 dès lors que le régime en cause ne satisfait pas à l'exigence de « qualité de la loi » et est incapable de maintenir l'« ingérence » dans ce que qui est « nécessaire dans une société démocratique » et constate une violation de l'article 8 (§ 388)."

d'une autorité indépendante.[115] Ainsi les Etats-Unis ne sont pas les seuls concernés par des sanctions sur leur politique de renseignement, l'arrêt Schrems II a mis en lumière l'analyse d'une protection des données cohérente, puis la CJUE est restée dans la continuité de cet arrêt dans son arrêt du 6 octobre 2020, comme la CEDH l'était déjà auparavant contre le Royaume-Uni.

Les Etats européens ne sont pas exempts de condamnations au sujet de la protection des données face à la sécurité nationale. La France notamment est critiquée et pourrait encore faire l'objet de nouvelles condamnations. En effet deux nouveautés en matière de protection des données ont eu lieu : une décision du conseil constitutionnel du 20 mai 2021 appuyant sur le défaut de conformité à la constitution et à la Loi informatique et libertés qui transpose le RGPD de certaines dispositions de la Loi pour une sécurité globale préservant les libertés[116] ; et une question prioritaire de constitutionnalité posée par la Quadrature du Net contre l'article L 863-2 du code de la sécurité intérieure[117]. Il s'agit dans ces deux cas de revendiquer la cohérence dans la protection des données ayant pour conséquence une limite dans l'ingérence publique sur les données des citoyens. Comme l'énonce La Quadrature du Net dans sa QPC : "*L'article L. 863-2 du code de la sécurité intérieure ne fixe aucune condition relative à l'exploitation, la conservation ou la destruction des renseignements collectés et partagés sur le fondement de cet article, ni pour le partage des 10 extractions et des transcriptions réalisées à partir de ces renseignements « bruts ». Si le titre V du livre VIII du code de la sécurité intérieure dresse bien la liste des techniques de recueil de renseignement et prévoit, pour chacune d'entre elles, différents régimes d'autorisation, de collecte, d'exploitation et de conservation des renseignement, extractions et transcriptions légalement autorisées, le partage de ces données opéré en vertu de l'article L. 863-2 a pour effet d'affranchir les services de renseignement de tout encadrement législatif ou réglementaire.*" (point 31) De ces termes, la notion de continuité dans la protection ressort bien puisque selon l'association il faudrait que les conditions de collectes de données dans le cadre de l'article soient fixées puisqu'il faut toujours fonder un traitement de données selon le RGPD et la jurisprudence

[115]CEDH 13 sept. 2018, Big Brother Watch et a. c. Royaume-Uni, nos 58170/13, 62322/14 et 24960/15§466 : Consequently, the Government have conceded that Part 4 of the IPA is incompatible with EU law because access to retained data was not limited to the purpose of combating "serious crime"; and access to retained data was not subject to prior review by a court or an independent administrative body. Following this concession, the High Court ordered that the relevant provisions of the IPA should be amended by 1 November 2018 (see paragraph 196 above).

[116] Décision n° 2021-817 DC du 20 mai 2021

[117] Conseil d'Etat section du contentieux - question prioritaire de constitutionnalité n° 431980 - La quadrature du Net contre L 863-2 CSI

européenne, et surtout il faut que les dispositions relatives au renseignement dans un même pays soient cohérentes pour qu'il n'y ait pas de failles de protection. Enfin, pour prendre un exemple de la décision du conseil constitutionnel du 20 mai 2021, l'article 48 de la pour la sécurité globale a été jugé inconstitutionnel car "*le législateur n'a pas assuré une conciliation équilibrée entre, d'une part, les objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions, et, d'autre part, le droit au respect de la vie privée.*" (point 148) En effet, si l'on veut être cohérent dans la protection des données il est nécessaire de donner l'information aux personnes concernées quel que soit le traitement de données (articles 12, 13 et 14 du RGPD) et ici les exceptions à cette transparence dans le cadre des caméras embarquées rendaient cette dernière inexistante.[118] Avant cela, on peut encore citer un arrêt du Conseil d'Etat du 18 mai 2020 qui a interdit la surveillance par drone dans un contexte de crise sanitaire car elle est irrespectueuse du droit fondamental à la vie privée. Dans cet arrêt, Le Professeur A. Bouveresse indique que le juge donne une alternative au cadre réglementaire qui est une "*amélioration technique des drones « de nature à rendre impossible, quels que puissent en être les usages retenus, l'identification des personnes filmées* » (pt 19)".[119] Ainsi, que les garanties à la protection de la vie privée soient légales ou techniques il faut qu'elles soient présentes et elles ne le sont pas toujours, quel que soit le pays considéré.

Pour résumer, les différentes cours, internes et internationales, cherchent à placer le curseur au bon endroit pour équilibrer sécurité et protection des des données personnelles dans un discours empreint d' "*une forme d'égalité des armes"* tout en ayant à l'esprit que "*l'amoncellement des menaces ne doit être ni surestimé ni sous-estimé*"[120]. En effet l'ingérence des services de renseignement doit être proportionnée à la menace qui doit en conséquence être qualifiée et prévisible. Cependant les Etats sont plus enclins à se donner une

[118] Décision n° 2021-817 DC du 20 mai 2021 - Point 144 : *les dispositions contestées prévoient que les caméras embarquées équipant les moyens de transport précités peuvent capter, enregistrer et transmettre des images au sein de ces véhicules, sur la voie publique ou dans des lieux ouverts au public, y compris, le cas échéant, de l'intérieur des immeubles ainsi que de leurs entrées. D'autre part, outre une information générale du public par le ministre de l'intérieur, le législateur n'a prévu pour seule information spécifique du public que l'apposition d'une signalétique lorsque les véhicules sont équipés de caméras. Cette dernière information n'est pas donnée lorsque « les circonstances l'interdisent » ou lorsqu'elle « entrerait en contradiction avec les objectifs poursuivis ». De telles exceptions permettent de déroger largement à cette obligation d'informer et, plus particulièrement, en matière d'investigations pénales dès lors qu'une telle information est le plus souvent en contradiction avec l'objectif de recherche des auteurs d'infractions et de constatation de ces dernières. Enfin, les images captées peuvent être transmises en temps réel au poste de commandement du service utilisateur.*

[119] BOUVERESSE Aude - Surveillance par drones : quand la technique évite les atteintes aux droits - in RTD Eur. 2020 p.956

[120] Blog de Daniel Mainguy - Chronique de droit des militaires Généralités 5. Les limites de la collecte de métadonnées par les agences de renseignement - 3 Février 2021

plus grande marge de pouvoir de collecte de données afin d'être plus libres dans la mise en place de leurs politiques sécuritaires. Cette pratique des lois sécuritaires européennes ne va pas avec la cohérence dans la protection des données qu'a voulu pointer la Cour de Justice dans son arrêt Schrems II. Cette continuité est aussi contestable en matière de transfert de données.

Section 2 : Les transferts, entre protection et intérêts commerciaux

La récente décision d'adéquation envers le Japon du 23 janvier 2019[121] mérite qu'on y porte attention afin de mettre en pratique les principes de référence pour considérer qu'une législation apporte un niveau de protection "essentiellement équivalent"[122], de voir qu'il a fallu du temps et des changements pour que la commission accepte de considérer ce niveau adéquat, et enfin de la mettre en rapport avec le Privacy Shield (A). De plus, on peut contester la force de clauses contractuelles type pour lutter contre des systèmes de surveillance étrangers (B)

[121] Décision d'adéquation (UE) 2019/419 de la commission du 23 janvier 2019 constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le Japon en vertu de la loi sur la protection des informations à caractère personnel [notifiée sous le numéro C(2019) 304]

[122] Considérant 104 du RGPD : *"Eu égard aux valeurs fondamentales sur lesquelles est fondée l'Union, en particulier la protection des droits de l'homme, la Commission devrait, dans son évaluation d'un pays tiers, d'un territoire ou d'un secteur déterminé dans un pays tiers, prendre en considération la manière dont un pays tiers déterminé respecte l'état de droit, garantit l'accès à la justice et observe les règles et normes internationales dans le domaine des droits de l'homme, ainsi que sa législation générale et sectorielle, y compris la législation sur la sécurité publique, la défense et la sécurité nationale ainsi que l'ordre public et le droit pénal. Lors de l'adoption, à l'égard d'un territoire ou d'un secteur déterminé dans un pays tiers, d'une décision d'adéquation, il y a lieu de tenir compte de critères clairs et objectifs, telles que les activités de traitement spécifiques et le champ d'application des normes juridiques applicables et de la législation en vigueur dans le pays tiers. Le pays tiers devrait offrir des garanties pour assurer un niveau adéquat de protection essentiellement équivalent à celui qui est garanti dans l'Union, en particulier quand les données à caractère personnel sont traitées dans un ou plusieurs secteurs spécifiques. Plus particulièrement, le pays tiers devrait assurer un contrôle indépendant effectif de la protection des données et prévoir des mécanismes de coopération avec les autorités de protection des données des États membres, et les personnes concernées devraient se voir octroyer des droits effectifs et opposables ainsi que des possibilités effectives de recours administratif et juridictionnel."*

A. Une adéquation révélatrice avec le Japon

La décision d'adéquation en faveur du japon est intéressante car elle a eu lieu après l'entrée en vigueur du RGPD, ce qui fait d'elle une application directe des nouveaux critères d'adéquation assurant la protection des données dans les transferts. En 2018, le Parlement Européen disait à ce sujet que si une décision d'adéquation était prise avec le Japon elle serait peut-être un modèle pour les prochaines.[123] La chronologie des événements avant d'en arriver à la décision finale de la commission est pertinente à retracer. La loi japonaise n'était pas comparable au RGPD au départ et donc elle a dû faire l'objet d'une modification faisant entrer de nouvelles règles de protection des données afin que la commission accepte de promulguer cette décision. Le but étant d'atténuer les différences entre les deux systèmes de droit européen et japonais. L'APPI, loi de protection des données au Japon a donc été modifiée en 2015 et en 2018 des normes additionnelles ont été ajoutées, rendant possible une analyse approfondie du système mis en place pour décider d'une liberté des transferts des données européennes vers cet Etat tiers. L'étude de la commission a ainsi porté en premier lieu sur une "*protection de base*" des données conforme au RGPD et ensuite à son application face aux lois de surveillance japonaises.

La Commission, après avis du CEPD, a considéré plusieurs aspects de la législation japonaise pour fonder sa décision d'exécution. Tout d'abord, dans ses considérants 7 et 9, elle a retenu le fait que la vie privée est protégée par l'article 13 de la Constitution japonaise de 1946 précisé par un arrêt de la Cour suprême de 1969.[124] Une décision de 2008 ensuite a confirmé sur ce sujet que ce droit constitutionnel induit "la liberté d'empêcher que ses informations à caractère personnel soient divulguées à un tiers ou rendues publiques sans raison valable".[125] Ainsi il y a bien une protection générale de la privée établie par les textes et la jurisprudence japonaise. Plus précisément, dans le cadre de la protection des données personnelles, le Japon a adopté quelques lois le 30 mai 2003 qui apportent un cadre prévisible

[123] Résolution du Parlement européen du 13 décembre 2018 sur l'adéquation de la protection des données à caractère personnel assurée par le Japon (2018/2979(RSP))- Journal Officiel du 13 novembre 2020 - Numéro C388 - Page 0150 - point 27 :" *la décision d'adéquation, si elle est adoptée, peut en outre attirer l'attention du monde entier sur les avantages extrêmement concrets qu'offre la convergence vers les normes rigoureuses de l'Union en matière de protection des données; souligne, à cet égard, l'importance de cette décision d'adéquation, susceptible de faire jurisprudence pour de futurs partenariats avec d'autres pays qui ont adopté un cadre juridique moderne en matière de protection des données"*

[124] Cour suprême, arrêt du Grand Bench du 24 décembre 1969, Keishu vol. 23, no 12, p. 1625. L'article 13 de la Constitution évoque seulement le droit à la vie, à la liberté et à la poursuite du bonheur ; partant de là l'apport de cet arrêt de la cour suprême est de garantir que le droit à la vie privée est vu comme un droit constitutionnel.

[125] Cour suprême, arrêt du 6 mars 2008, Minshu vol. 62, no 3, p. 665.

et donc de la sécurité juridique en la matière[126]. L'APPI telle que modifiée par la loi de 2015 a fait entrer de nouvelles garanties dans le droit positif telle que la création d'une autorité de contrôle indépendante (PPC) pour assurer l'efficience des règles de protection des données. Ces éléments de fait donnent une vue appréciable pour considérer qu'à priori le Japon offre un gage de respect de la vie privée et d'un traitement licite des données. Après avoir vérifié cette "protection de base"[127], la commission a demandé des garanties supplémentaires au Japon pour réduire les différences entre les deux réglementations, par exemple elle a demandé à bien encadrer les transferts ultérieurs de données européennes, l'accès aux données par les autorités répressives pour assurer la sécurité nationale et à mettre en place un système spécifique pour les plaintes des européens sur leurs données.[128] Malgré tout cela il

[126] Considérant 9 de la Décision d'adéquation 2019/419 : "*Le 30 mai 2003, le Japon a adopté une série de lois dans le domaine de la protection des données:*

- *la loi sur la protection des informations à caractère personnel (APPI),*
- *la loi sur la protection des informations à caractère personnel détenues par des instances administratives (APPIHAO),*
- *la loi sur la protection des informations à caractère personnel détenues par des agences administratives intégrées (APPI-IAA)."*

[127] Les considérants 39 et suivants de la décision d'adéquation 2019/49 traitent ensuite du contenu des règles considérées comme essentielles, vérifiant à chaque fois leur existence et leur condition d'application. Par exemple les articles 15 et 16 de l'APPI édictent la règle de la limitation du traitement des données à la finalité précise qui est poursuivie ou à une finalité étroitement et raisonnablement liée à celle qui est définie, ce qui implique aussi le respect du principe de minimisation des données puisque l'article 16 paragraphe 1 de l'APPI interdit le traitement d'informations à caractère personnel au-delà de la «mesure nécessaire pour atteindre une finalité d'utilisation». La licéité et la loyauté du traitement sont définies à l'article 17 de la même loi, ainsi un traitement ne peut être effectué après avoir trompé la personne concernée et donc il faut privilégier le consentement de cette dernière pour fonder un traitement. Pour que le consentement soit valide il faut bien entendu que certains critères de transparence soient remplies, et c'est le cas dans l'article 18 qui demande que les personnes concernées soient informées sur la finalité d'utilisation des informations à caractère personnel. L'article 19 de la loi oblige le responsable de traitement (OETIP) à supprimer les données collectées lorsqu'elles ne sont plus nécessaires à la finalité du traitement. Les articles 20 et 21 de l'APPI reprennent le principe de sécurité des données du RGPD en obligeant l'OETIP à assurer une «supervision nécessaire et appropriée» à des fins de contrôle de la sécurité. En sachant que la perte ou le vol de données peut entraîner la prison pour celui-ci. De plus la loi japonaise ouvre une distinction selon que les données sont sensibles ou non, ainsi il est fait mention de données à caractère personnel "nécessitant des précautions particulières" qui renvoit à la liste des données jugées sensibles par l'article 9 du RGPD.

[128] Avant que la Commission n'adopte sa décision d'adéquation, le Japon a mis en place des garanties supplémentaires permettant de s'assurer que les données transférées de l'Union vers le Japon bénéficient de garanties de protection conformes aux normes européennes. Ces garanties comprennent:

- Un ensemble de règles (règles supplémentaires) qui permettront de réduire certaines différences entre les deux systèmes de protection des données. Ces garanties supplémentaires renforceront, par exemple, la protection des données sensibles, l'exercice des droits individuels et les conditions selon lesquelles les données de l'UE peuvent être transférées ultérieurement depuis le Japon vers un autre pays tiers. Ces règles supplémentaires seront contraignantes pour les entreprises japonaises qui importent des données de l'UE et pourront être invoquées par l'autorité indépendante japonaise de protection des données et les juridictions japonaises.
- Le gouvernement japonais a également fourni des assurances à la Commission en ce qui concerne l'accès aux données par les autorités publiques japonaises aux fins des procédures pénales et de la sécurité nationale, garantissant que toute utilisation des données à caractère personnel à ces fins serait limitée à ce qui est nécessaire et proportionnée, et soumise à des mécanismes de surveillance et de recours indépendants.

reste des différences entre les deux systèmes mais comme il n'est pas nécessaire que les systèmes soient similaires pour être substantiellement équivalent, cela ne fait pas obstacle à une protection des données adéquate. "*Ainsi, la Cour Suprême japonaise n'a pas reconnu les principes du droit à l'oubli (arrêt de juillet 2018), du droit au contrôle de ses propres informations ou encore la possibilité pour un utilisateur d'engager une procédure judiciaire afin d'avoir accès à ses informations personnelles*"[129] et cela n'a pas empêché à la commission de considérer que les systèmes étaient "substantiellement équivalents" selon l'article 45 interprété par l'arrêt Schrems[130]. En effet les éléments considérés comme essentiels par le groupe de travail "article 29" sont présents dans la législation japonaise, notamment l'autorité de contrôle indépendante et les voies de recours pour les personnes concernées.[131] C'est pourquoi le considérant 119 de la décision d'adéquation explique que "*le droit japonais prévoit plusieurs limitations de l'accès aux données à caractère personnel et de l'utilisation de ces données à des fins répressives, ainsi que des mécanismes de surveillance et de recours qui offrent des garanties suffisantes pour que lesdites données soient protégées de manière efficace contre les interventions illicites et le risque d'abus.*"

Maintenant, concernant les garanties essentielles dans les pays tiers en matière d'application des lois et d'accès pour raison de sécurité nationale afin de limiter les ingérences dans les droits fondamentaux (chapitre 4 des critères de référence pour l'adéquation du groupe de travail "article 29"), le Parlement Européen avait relevé en 2018

- Un mécanisme de traitement des plaintes visant à enquêter sur les plaintes des Européens concernant l'accès à leurs données par les autorités publiques japonaises, et à les traiter. Ce nouveau mécanisme sera géré et contrôlé par l'autorité indépendante japonaise de protection des données.

[129] Source : La direction générale du Trésor - La protection des données personnelles au Japon - Rédigé par DG Trésor • Publié le 08 mai 2019

[130] Considérant 175 de la décision d'adéquation 2019/419 : "Compte tenu de ces éléments, la Commission conclut au respect de la norme en matière d'adéquation prévue à l'article 45 du règlement (UE) 2016/679, interprétée à la lumière de la charte des droits fondamentaux de l'Union européenne, en particulier dans l'arrêt Schrems."

[131] les articles 40 et 41 de l'APPI donnent compétences à une autorité de contrôle indépendante (PPC) et ensuite les articles 32 et 17 de la Constitution japonaise l'article 17 de la Constitution garantissent des recours individuels. La PPC (Personal Information Protection Commission) peut demander toute information qu'elle juge nécessaire aux opérateurs de traitement de données, elle peut effectuer des vérifications sur place en envoyant des agents dans les bureaux de ces derniers afin de vérifier le bon fonctionnement interne de protection des données. De plus, selon l'article 42 de l'APPI, la PPC peut ordonner la cessation d'une violation si elle découvre que l'opérateur va à l'encontre des règles de fond évoquées ci-dessus tout comme la CNIL en France. Le même article donne aussi le pouvoir à l'autorité de contrôle de prononcer toute mesure obligatoire afin de remédier à la violation de données après sa cessation. A noter que la sanction est dure si l'opérateur ne satisfait pas à l'astreinte de la commission de contrôle, en effet l'article 84 de l'APPI qualifie ce manquement d'une infraction pénale qui peut entrainer une peine d'un an de prison. Les personnes individuelles ont aussi la possibilité d'effectuer des recours si leurs données sont mal utilisées par les opérateurs de traitement et dans ce cas ceux-ci doivent réagir le plus rapidement possible pour traiter les plaintes, comme l'énonce l'article 35 de l'APPI.

que “les opérateurs économiques peuvent également, à leur gré, transférer des données aux autorités répressives”[132] et a demandé à la commission de statuer sur la point de savoir si c’était conforme à la réglementation européenne (point 23 de la résolution du Parlement européen du 13 décembre 2018 sur l'adéquation de la protection des données à caractère personnel assurée par le Japon (2018/2979). La commission répond dans les considérants 151 et suivants en montrant que lorsque les autorités publiques japonaises accèdent aux données à des fins de sécurité nationale, cela est encadré par la Diète, le bureau de l’inspecteur général et les commissions préfectorales de sûreté publique pour la police. Ainsi il y a un encadrement au niveau des autorités, mais aussi au niveau des données qu’il est possible de recueillir. Le considérant 156 de la décision d'adéquation informe en effet que «la collecte et le traitement des informations se font uniquement dans la mesure nécessaire à l’exécution des tâches spécifiques de l’autorité publique compétente et en fonction des menaces spécifiques». En conséquence, «cela exclut la collecte massive et indifférenciée ou l’accès à des données à caractère personnel pour des raisons de sécurité nationale». De cette manière, et grâce à ces diverses encadrement, il est possible de considérer que les données ont une protection substantiellement équivalente quand elles sont transférées au Japon. Cette affirmation est à tempérer puiqu’on a déjà connu les cas du Safe Harbor et du privacy Shield qui, sans être des décisions d’adéquation, prévoyaient des droits similaires pour protéger les données des individus et cela n’a pas suffit.[133] Pourtant M. Andrus Ansip, vice-président de la Commission européenne, avait pu dire à l’époque : “*Nous nous sommes accordés sur un nouveau cadre solide pour les flux de données vers les États-Unis. Nos concitoyens peuvent avoir la certitude que leurs données à caractère personnel seront bien protégées*.”[134] Il est certain que les considérations d’intérêts commerciaux entrent en ligne de compte et permettent de considérer qu’un Etat tiers offre une protection essentiellement équivalente

[132] Quatre organismes publics sont habilités à recueillir des informations électroniques auprès des acteurs économiques japonais pour des raisons de sécurité nationale :

- le bureau d’analyse et de renseignement du gouvernement (Cabinet Intelligence & Research Office : CIRO)
- le ministère de la défense
- la police (la police nationale et la police préfectorale)
- l’agence de renseignement en matière de sécurité publique (Public Security Intelligence Agency : PSIA)

[133] Le Safe Harbor est mort… Peut-on dire « vive le Privacy Shield » (le bouclier de protection de la vie privée) ? Par Squire Patton Boggs, le 3 février 2016

[134] Communiqué de Presse de la Commission européenne - 2 février 2016 : La Commission européenne et les États-Unis s’accordent sur un nouveau cadre pour les transferts transatlantiques de données, le «bouclier vie privée UE-États-Unis»

alors qu'au fond ce n'est pas le cas et que les lois de surveillance et de collecte de données pour la sécurité de cet Etat ne permettent pas de respecter une protection cohérente des données. C'était le cas pour les Etats-Unis et le Privacy Shield, ça pourrait l'être avec le Japon du fait de sa loi anti-conspiration[135]. On retrouve en tout cas le même type de discours de la part de Mme Věra Jourová, commissaire chargée de la justice, des consommateurs et de l'égalité des genres : "*Cette décision d'adéquation donne naissance au plus grand espace au monde de flux sécurisés de données. Les Européens bénéficieront de normes strictes en matière de protection de la vie privée lorsque leurs données seront transférées vers le Japon*"[136]

On voit le temps qu'il a fallu pour que l'Union Européenne et le Japon se mettent d'accord sur la réglementation applicable et les garanties supplémentaires à apporter aux données européennes, pour que l'analyse et le bilan de la protection japonaise soient effectués afin de parvenir à une conclusion positive. Cela donne une relative force à la décision d'adéquation mais fait douter par la même occasion de la capacité des clauses contractuelles types ou des autres moyens pour assurer une continuité similaire dans la protection lors des transferts de données.

B. Le pragmatisme des clauses contractuelles types

L'article 45 du RGPD prévoit les transferts fondés sur une décision d'adéquation et le met en avant par rapport aux transferts fondés sur d'autres moyens, édictés dans l'article 46 du RGPD. Dans ce dernier article, il est donné la possibilité de se fonder sur des clauses contractuelles types, ceci étant confirmé dans l'arrêt Schrems II. Cependant on peut douter de l'efficacité de leur protection.

La protection des données lue à la lumière de la Charte des droits fondamentaux et des arrêts Schrems I et Schrems II a acquis un aspect cohérent et continu, ou du moins tend à

[135] Global Voices - La très controversée loi anti-conspiration japonaise adoptée par le parlement Nevin Thompson (traduction Babusha Verma) - 19 juin 2017 / Journal du Geek - Avec sa nouvelle loi sur la surveillance, le Japon prend des airs de Minority Report - 20 juin 2017 / Mediapart - Au Japon, une loi pour «punir jusqu'aux pensées des gens» - Frederic Ojardias - 21 octobre 2017

[136] Communiqué de presse de la commission européenne - 23 janvier 2019 - La Commission européenne adopte une décision d'adéquation concernant le Japon, donnant naissance au plus grand espace de flux sécurisés de données au monde

l'obtenir. En effet l'arrêt Schrems II a bien affirmé que quel que soit la base sur laquelle un transfert est effectué (CCT, Décision d'adéquation etc.) il faut que le même niveau de protection "essentiellement équivalent" soit assuré. Ainsi les obligations de sécurité sont mises à la charges des parties aux transferts. L'importateur doit "*mettre en œuvre les procédures permettant de garantir la sécurité du transfert et du traitement des données, de respecter les finalités du transfert, de désigner le service compétent pour répondre aux demandes de l'exportateur, des personnes concernées ou de l'autorité nationale de régulation.*[137]" Quand l'exportateur doit *"vérifier que l'importateur est en mesure de se conformer aux obligations légales*"[138] Ainsi pour chaque transfert fondé sur des clauses contractuelles types, il faut vérifier au cas par cas si le mécanisme est adéquat par rapport au but de protection des données défini par l'arrêt Schrems II reprenant l'arrêt Schrems I, en lien avec l'objectif de protection substantiellement équivalent de l'article 45 du RGPD comme cela a été vu dans la première partie. Dans cette idée, le Comité européen de la protection des données (CEPD) a donné ses recommandations pour guider les transferts fondés sur des clauses contractuelles types et en conformité avec le RGPD et la Charte des droits fondamentaux revus à la lumière des arrêts Schrems.[139] L'idée majeure du texte étant de donner des clés de sécurisation supplémentaire lorsque l'Etat importateur de données n'offre pas des garanties adéquates. Il peut s'agir de recours à des moyens techniques de protection comme le chiffrement, la pseudonymisation, etc. ou des mesures complémentaires contractuelles ou organisationnelles.[140] Le manque de garanties sur la protection des données dans un Etat tiers pose en effet problème et on attend de l'exportateur de données qu'il soit digilent quant à la protection supplémentaire à apporter aux données mais cela ne fait pas tout. Les clauses contractuelles types ne lient pas les Etats mais les parties seulement et donc elles ne peuvent pas être un poids assez important contre des lois de surveillance dans toutes les situations. La nécessité des transferts de données et les intérêts commerciaux sous-jacents l'emportent donc encore sur la cohérence dans leur protection.

Dans un commentaire sur la décision Schrems II, L'avocate Nathalie Metallinos a repris les propos de l'avocat général Henrik Saugmandsgaard Øe et a pu affirmer : "*dans le*

[137] Source : Dalloz - Praxis Cyberdroit - Chapitre 115 - Transfert des données à caractère personnel hors de l'Union européenne – Christiane Féral-Schuhl – 2020-2021 - section 3
[138] Cf note précédente
[139] EDPB : Recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE - Adoptées le 10 novembre
[140] Source Dalloz : RTD Eur. Chronique Droit européen du numérique - Les enjeux de la surveillance numérique – Brunessen Bertrand – RTD eur. 2021. p. 175

cas des États-Unis l'évaluation à effectuer est d'analyser si les clauses contractuelles types sont de nature à permettre la continuité du niveau de protection nonobstant le fait que les autorités américaines ne sont pas liées par les clauses contractuelles types et qu'elles peuvent de ce fait accéder aux données à caractère personnel transférées. Les clauses contractuelles types ne sont donc pas invalides du seul fait que les lois de surveillance américaines permettent l'accès aux données à caractère personnel transférées (pt 127). Toute autre interprétation aurait pour effet de remettre en cause la possibilité même de reposer sur des mécanismes contractuels pour assurer un niveau de protection adéquat (pt 121). L'approche prônée par l'Avocat général est ainsi basée sur la nécessité de faire preuve de pragmatisme et de ne pas anéantir l'un des mécanismes les plus utilisés pour transférer des données en dehors de l'Union européenne, notamment depuis l'invalidation du Safe Harbor, évitant de placer les organismes exportateurs dans une impasse (V. RAE 2016/2, études, p. 265, nos obs., spéc. p. 272).''[141] Entre le fait que les Etats ne sont pas liés par les clauses contractuelles types ; que les organismes privés ne peuvent pas faire le poids contre les autorités de surveillance qui exigent le transfert des données personnelles conservées par ceux-ci ; et que même si des lois de surveillance permette l'accès aux données le transfert est possible sur le fondement de telles clauses pour assurer plus de souplesse, on voit bien que le niveau de protection est moins fort que dans le cadre de transferts fondés sur une décision d'adéquation. Car pour ces derniers, les Etats ont discuté, ont pris des mesures complémentaires pour que, même s'il est toujours possible à des lois de surveillance de prévoir un accès aux données, les traitements soient véritablement encadrés.

[141] Source Lexis Nexis - Transferts de données - Perspectives de sauvetage des « clauses contractuelles types » par la CJUE, mais à quel prix ? - Commentaire par Nathalie METALLINOS - Communication Commerce électronique n° 4, Avril 2020, comm. 35

Conclusion

L'arrêt Schrems II donne une vision cohérente de la protection des données personnelles qui tend à la renforcer. Cette vision était déjà visible dans les différents textes réglementaires, dans les directives, dans les jugements même, mais elle est véritablement devenue prépondérante depuis la décision Schrems II. Ce n'est pas anodin car la continuité de la protection, que l'on passe d'un traitement de données commercial à un traitement de données à des fins de sécurité publique, permet de se référer non plus à un texte mais à l'idée d'un texte qui en principe ne pourrait pas s'appliquer à une matière précise (le RGPD ou la directive e-privacy par exemple qui ne s'appliquent pas en matière de sécurité publique et de sûreté de l'Etat).

Cependant en pratique la continuité dans la protection des données est encore à améliorer lorsque des lois de surveillance pour la sécurité et la paix publique surviennent, que l'on soit au sein des Etats Membres ou dans le cadre des transferts de données. En effet les Etats considèrent que la sécurité publique reste une matière qui leur est propre et n'aiment pas être jugés sur les moyens qu'ils utilisent pour l'assurer. De plus, en ce qui concerne les transferts, la volonté pragmatique de vouloir faire commerce et avoir des relations d'affaires avec un Etat tiers entraîne nécessairement un amoindrissement de la protection des données européennes transférées, puisque la notion de vie privée n'est pas la même selon chaque culture, malgré l'attention portée au niveau "*essentiellement équivalent*" de protection dans l'État dans lequel les données sont transférées.

Le conflit entre la protection des données personnelles, la vie privée, et l'ingérence massive des lois de surveillance n'est donc pas terminée, en interne ou à l'international, mais la voie est en train de se tracer. Pour reprendre les mots du Professeur Kuner dans une interview de 2018[142] : "*la seule autre solution serait que les pays parvienne à un consensus mondial sur la confidentialité des données, mais cela est peu probable dans un avenir proche... Je pense donc que de nombreux domaines de la confidentialité des données resteront controversés, et je m'attends à ce que les choses deviennent plus désordonnées avant de s'améliorer*".

[142] KUNER Christopher : Interview with Goldman Sachs about the EU General Data Protection Regulation (GDPR), April 2018

Bibliographie

I. OUVRAGES

- FERAL-SCHUHL - Cyberdroit 2020-2021, Le droit à l'épreuve de l'Internet - 8e édition - 2020 - Ed. Dalloz
- GEFFRAY Edouard; GUERIN-FRANCOIS Alexandra; AÏT-EL-KADI Zéhina; MAXIMIN Nathalie - *Code de la protection des données personnelles 2021* - 3e édition - 2020 - Ed. Dalloz
- TÜRK Pauline ; VALLAR Christian - *La souveraineté numérique*, *le concept les enjeux* - Ed. Mare et Martin - 2018
- BASDEVANT Adrien ; MIGNARD Jean-Pierre - L'empire des données, essai sur la société, les algorithmes et la loi - Ed. Don Quichotte - 2018

II. ARTICLES ET CHRONIQUES

- ANDRIANTSIMBAZOVINA Joël - *La surveillance de masse des communications et des données au nom de la lutte contre le terrorisme nécessite des garanties suffisantes contre les abus* - in la Gazette du Palais - n°09 - page 44 - 01/03/2016
- BONNEVILLE Philippe ; GÄNSER Christian ; MARKARIAN Sophie ; ILJIC Anne - *Chronique de jurisprudence de la CJUE* - in AJDA 2021. p. 387
- BOUVERESSE Aude - *Surveillance par drones : quand la technique évite les atteintes aux droits* - in RTD Eur. 2020 p.956
- BRUNESSEN Bertrand ; SIRINELLI Jean - *Schrems II : on prend les mêmes et on recommence* - in Dalloz IP/IT 2020. p.640
- BRUNESSEN Bertrand - *Chronique Droit européen du numérique : Les enjeux de la surveillance numérique* - in RTD eur. 2021. p. 175
- CRICHTON Cécile - *Transfert de données vers les USA : l'arrêt Schrems II* - in Dalloz actualités - le 22 juillet 2020
- CRICHTON Cécile - *Précisions sur la conservation de données aux fins de la lutte contre la criminalité* CJUE, 2 mars 2021 - Dalloz IP/IT n°01 29/02/2021- page 46

- DANIS-FATÔME Anne - *La protection des données personnelles résiste à la surveillance générale qu'imposerait la lutte contre le terrorisme* - in Communication Commerce électronique n° 4, Avril 2020, comm. 36
- DEROUDILLE Alexis - *L'arrêt Schrems II, vers une résolution de l'équation transatlantique ?* in Rev. UE 2021. p. 144
- HADDAD Sophie ; CASANOVA Antoine ; DUBOIS Nina - *Arrêt "Schrems 2", la cour de justice de l'Union Européenne invalide le système du privacy shield* - in Village Justice - le 7 août 2020
- HATZOPOULOS Vassilis - *Économie collaborative : vers un cadre de la régulation des plateformes ?* - Répertoire de droit européen chap. 1 ; sect. 3 ; art. 3 ; 41 - Janvier 2020 (actualisation : Octobre 2020)
- LAVRIC Sabrina - *Surveillance de sécurité : le Royaume-Uni condamné pour son système d'interception et d'obtention de données* - in Dalloz actualités - 4 octobre 2018
- MAISON-ROUGE (de) Olivier - *Le droit français du renseignement* - in Répertoire IP/IT et communication - juillet 2019
- MARTIAL-BRAZ Nathalie - *Transfert des données hors UE : stop ou encore ?* - in Revue de Droit bancaire et financier n° 6, Novembre 2020, comm. 147
- METALLINOS Nathalie - *Transferts de données : Perspectives de sauvetage des « clauses contractuelles types » par la CJUE, mais à quel prix ?* - in Communication Commerce électronique n° 4, Avril 2020, comm. 35
- MONTECLER (de) Marie-Christine - *Techniques de renseignement : quand le Conseil d'État invite la CJUE à revoir sa jurisprudence* - in Dalloz Actualités - Le 7 septembre 2018
- PERRAY Romain ; MCDERMOTT Will ; AARPI Emery - *Introduction générale et champ d'application de la réglementation relative à la protection des données personnelles* - in Fasc. 274-10 : Informatique / 9 avril 2019 - Point clé n°8
- SAURON Jean-Luc ; GUYOMAR Mattias - *La protection des données personnelles à l'aune du droit au respect de la vie privée et familiale de l'article 8 de la convention* - in Gaz. Pal. 3 déc. 2019, n° 364m9, p. 15
- SCHWARTZ M. (P), PEIFER (K.N), « Transatlantic Data Privacy Law », The George Town Law Journal, volume 106, 2017, pp. 115 à 179.
- TAMBOU Olivia - Propos libres autour de l'invalidation par la CJUE de la décision Safe Harbor - in Dalloz actualités - 9 octobre 2015

- THARD-JALLU Cécile ; JOB Jean-Marie ; MINTZ Simon - *Invalidation de l'accord Safe Harbor par la CJUE : portée, impacts et premiers éléments de solution* - in Dalloz IP/IT 2016. p.26

III. THESES ET MEMOIRES

- BEGNY Laurélenn : *Règlement général sur la protection des données personnelles : vers une remise en cause du modèle français ?* - Mémoire - Université de Poitiers - 2017 - https://opac.cndp.ma/doc_num.php?explnum_id=55
- LONGHAIS Sylvain - *Le Privacy Shield : cadre juridique efficace ou accord politico-économique ?* - Mémoire - Université d'Aix-Marseille - 2019 - http://www.iredic.fr/wp-content/uploads/2020/04/longhais-s.-macopymoire-privacy-shield-2018-2019.pdf

IV. TEXTES, LOIS, DIRECTIVES, RÈGLEMENTS

☐ Textes européens

- 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).
- Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales telle qu'amendée par les Protocoles n° 11 et n° 14 - Rome, 4.XI.1950
- Charte des droits fondamentaux de l'Union Européenne (2000/C 364/01)
- Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)
- Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de

détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil

- Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»)
- Commission européenne, UE-US Privacy Shield, 2 février 2016
    - Communiqué de Presse de la Commission européenne - 2 février 2016 : La Commission européenne et les États-Unis s'accordent sur un nouveau cadre pour les transferts transatlantiques de données, le «bouclier vie privée UE-États-Unis»
- Groupe de travail "article 29" sur la protection des données - Document de travail établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes / Adopté le 28 novembre 2017 / Version révisée et adoptée le 6 février 2018
- EDPB : Recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE - Adoptées le 10 novembre
- Décision d'adéquation (UE) 2019/419 de la commission du 23 janvier 2019 constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le Japon en vertu de la loi sur la protection des informations à caractère personnel [notifiée sous le numéro C(2019) 304]
    - Communiqué de presse de la Commission européenne - *La Commission européenne adopte une décision d'adéquation concernant le Japon, donnant naissance au plus grand espace de flux sécurisés de données au monde* - 23 janvier 2019
- Résolution du Parlement européen du 13 décembre 2018 sur l'adéquation de la protection des données à caractère personnel assurée par le Japon (2018/2979(RSP))- Journal Officiel du 13 novembre 2020 - Numéro C388

☐ Textes français

- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique
- Loi n° 2015-912 du 24 juillet 2015 relative au renseignement
- Loi n° 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés

V. JURISPRUDENCES

☐ Jurisprudences de la CJUE

- CJUE grande chambre, du 6 octobre 2015, Schrems - aff. C-362/14
- CJUE 16 juill. 2020, DPC c. Facebook Ireland Ltd et M. Schrems, aff. C-311/18
- CJUE (grande chambre) 21 décembre 2016, affaires jointes C‑203/15 et C‑698/15, Tele2 Sverige AB contre Post- och telestyrelsen et Secretary of State for the Home Department contre Tom Watson e.a.
- CJUE 8 avril 2014 C-293/12 - Digital Rights Ireland et Seitlinger e.a.
- CJUE La Quadrature du Net e.a., affaires jointes C-511/18 et C-512/18 et Ordre des barreaux francophones et germanophone e.a., C-520/18 du 6 octobre 2020
    - Conclusions de l'avocat général - M. HENRIK SAUGMANDSGAARD ØE - présentées le 19 décembre 2019 (1) Affaire C‑311/18
    - Concl. av. gén. M. Campos Sanchez-Bordona, 15 janv. 2020, aff. jtes C-511/18 et C-512/18, La Quadrature du Net, French Data Network, Féd. des fournisseurs d'accès à Internet associatifs Igwan.net (C-511/18) c/ Premier ministre, garde des Sceaux, min. Justice, min. Intérieur, min. Armées et aff. C-623/17, Privacy International c/ Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Departement, Government Communications Headquarters, Security Service, Secret Intelligence Service
- CJUE grande chambre 2 mars 2021, Prokuratuur, aff. C-746/18

☐ Jurisprudences de la CEDH

- CEDH Klass et autres c. Allemagne (Req. 5029/71), 6 septembre 1978 / CEDH, Roman Zakharov c. Russie [GC], n° 47143/06, 4 décembre 2015 / CEDH Szabo et Vissy c. Hongrie (Req. 37/138/14), 12 janvier 2016
- CEDH 13 sept. 2018, Big Brother Watch et a. c. Royaume-Uni, nos 58170/13, 62322/14 et 24960/15§466
- CEDH, Roman Zakharov c. Russie [GC], n° 47143/06, 4 décembre 2015
- CEDH, 17 oct. 2019, nos 1874/13 et 8567/13, Lopez Ribalda et a. c/ Espagne, Linos-Alexandre Sicilianos, prés.

☐ Jurisprudence française

- CE 18 mai 2020, n° 440442, AJDA 2020. 1031, AJDA 2020. 1031
- Décision n° 2021-817 DC du 20 mai 2021
- Conseil d'Etat section du contentieux - question prioritaire de constitutionnalité n° 431980 - La quadrature du Net contre L 863-2 CSI
- CE 26 juill. 2018, req. n° 394922
- Décision n° 2020-801 DC du 18 juin 2020

VI. SITES INTERNET

- DAOUD Emmanuël ; PECRIAUX Océane - *Flash info : CJUE, 06 octobre 2020, données de connexion et sauvegarde de la sécurité nationale : l'exception confirme la règle* - 13/10/2020 - Site : Vigo - Disponible sur : https://vigo-avocats.com/legal-news/flash-info-cjue-06-octobre-2020-donnees-de-connexion-et-sauvegarde-de-la-securite-nationale-lexception-confirme-la-regle/
- Direction générale du Trésor Source - *La protection des données personnelles au Japon* - Publié le 08/05/2019 - Disponible sur https://www.tresor.economie.gouv.fr/Articles/2019/05/08/la-protection-des-donnees-personnelles-au-japon

- Journal du Geek - *Avec sa nouvelle loi sur la surveillance, le Japon prend des airs de Minority Report* - 20/06/2017 - Disponible sur : https://www.journaldugeek.com/2017/06/20/vous-avez-aime-minority-report-et-psycho-pass-le-gouvernement-japonais-aussi/#:~:text=D%C3%A9sormais%20les%20autorit%C3%A9s%20nipponnes%20pourront,terroristes%20qui%20planifient%20un%20crime.&text=Toute%20personne%20peut%20d%C3%A9sormais%20voir,par%20le%20projet%20de%20loi.
- KUNER Christopher : Interview with Goldman Sachs about the EU General Data Protection Regulation (GDPR), April 2018 - Disponible sur http://www.kuner.com/my-publications-and-writing/untitled/kuner-goldman-sachs-intervi.pdf
- La Quadrature du Net - *Partage de données : les services de renseignement violent la constitution* - Site de la Quadrature du Net - 01/03/2021 - Disponible sur : https://www.laquadrature.net/2021/03/01/partage-de-donnees-les-services-de-renseignement-violent-la-constitution/
- La Quadrature du Net - Loi Renseignement : le retour en pire - Site de la Quadrature du Net - 27/05/2021 - Disponible sur : https://www.laquadrature.net/2021/05/27/loi-renseignement-le-retour-en-pire/
- La Quadrature du net - Loi Sécurité globale adoptée : résumons - 16/04/2021 - Site de la Quadrature du Net - Disponible sur : https://www.laquadrature.net/2021/04/16/loi-securite-globale-adoptee-resumons/
- MAINGUY Daniel - Chronique de droit des militaires Généralités 5. Les limites de la collecte de métadonnées par les agences de renseignement - 03/02/2021 - https://www.daniel-mainguy.fr/2021/02/chronique-de-droit-des-militaires-generalites.html
- OJARDIAS Frederic - Au Japon, une loi pour «punir jusqu'aux pensées des gens» - 21/10/2017 - Disponible sur : https://www.mediapart.fr/journal/international/211017/au-japon-une-loi-pour-punir-jusqu-aux-pensees-des-gens?onglet=full
- REES Martin - *Loi Renseignement : la surveillance internationale examinée par les députés le 1er octobre* - 21/09/2015 - Site : Nextinpact - Disponible sur : https://www.nextinpact.com/article/19294/96574-loi-renseignement-surveillance-internationale-examinee-par-deputes-1er-octobre

- REES Marc - *Conservation des données : le gouvernement demande au Conseil d'État d'ignorer la justice européenne* - Site : Nextinpact - 03/03/2021 - Disponible surhttps://www.nextinpact.com/article/45724/conservation-donnees-gouvernement-demande-au-conseil-detat-dignorer-justice-europeenne
- SQUIRE PATTON BOGGS - Le Safe Harbor est mort… Peut-on dire « vive le Privacy Shield » (le bouclier de protection de la vie privée) ? - 03/02/2016 - Disponible sur : https://larevue.squirepattonboggs.com/le-safe-harbor-est-mort-peut-on-dire-vive-le-privacy-shield-le-bouclier-de-protection-de-la-vie-privee_a2797.html
- THARD-JALLU Cécile ; DELAUNAY Sophie - *La CJUE pose des limites à la surveillance de masse* - 27/10/2020 - De Gaulle, Fleurance & associés - disponible sur :https://www.degaullefleurance.com/la-cjue-pose-des-limites-a-la-surveillance-de-masse-2/#:~:text=La%20CJUE%20s'est%20prononc%C3%A9e,et%20Watson%20rendue%20en%202016.
- THOMPSON Nevin - *La très controversée loi anti-conspiration japonaise adoptée par le parlement* - 19/06/2017 - Disponible sur : https://fr.globalvoices.org/2017/06/19/211784/
- Vie publique, "*Renseignement français : quelle organisation et quel cadre légal ?*", publié le 15/01/2020 - Disponible sur : https://www.vie-publique.fr/eclairage/272339-renseignement-francais-quel-cadre-legal#:~:text=Le%20Conseil%20national%20du%20renseignement,le%20pr%C3%A9sident%20de%20la%20R%C3%A9publique.&text=La%20loi%20du%2024%20juillet,disposer%20d'un%20tel%20cadre.
- VITARD Alice - La justice européenne s'oppose à la transmission et la conservation généralisée des données de connexion - 06/10/2020 Site : l'usine digitale - https://www.usine-digitale.fr/article/la-justice-europeenne-s-oppose-a-la-transmission-et-la-conservation-generalisee-des-donnees-de-connexion.N1013189
- VOGIATZOGLOU Plixavra ; BERGHOLM Jenny - Privacy International & La Quadrature du Net: the latest on data retention in the name of national and public security – Part 1 - Disponible sur : https://www.law.kuleuven.be/citip/blog/privacy-international-la-quadrature-du-net-part-1/