Troisième tentative de réglementation visant à préserver les transferts transatlantiques de données : aperçu d'une analyse

Coline Dénériaz (MLaw student, Université de Fribourg)

Die EU-Kommission verabschiedet das Data Protection Framework (DPF) für die Übermittlung personenbezogener Daten von EU-Bürgern in die USA. Die Regelung soll nach der Ungültigerklärung von Safe Harbor und Privacy Shield die Datenübermittlung sicherer gestalten. Allerdings bleiben Bedenken hinsichtlich der US-Überwachung und Datenschutzstandards. Die Umsetzung und die praktische Anwendung des DPF werden in Frage gestellt, insbesondere werden die Aspekte des Legalitätsprinzips und der Verhältnismäßigkeit der staatlichen Maßnahmen der USA zum Schutz ihrer nationalen Sicherheit angezweifelt.

Introduction

Le 10 juillet 2023, la Commission européenne cristallise sa troisième tentative de règlementation de transfert des données de l'UE vers les États-Unis en adoptant une nouvelle décision d'adéquation : le *Data Protection Framework* (DPF). Cette adoption fait suite à l'invalidation par la Cour de Justice de l'Union Européenne (CJUE) des deux décisions précédentes : le *Safe Harbor*[1] (en vigueur de 2000 à 2015) et le *Privacy Shield*[2] (en vigueur de 2016 à 2020)[3].

La décision d'adéquation est l'un des dispositifs prévus par le Chapitre V du Règlement général sur la protection des données (RGPD) permettant le transfert de données personnelles de citoyens européens vers des États tiers[4]. À ce jour, seuls quinze États disposent d'une telle décision[5]. Les États-Unis sont à nouveau au bénéfice de cette reconnaissance d'adéquation, aussi longtemps que la CJUE n'invalide pas l'acte de la Commission. Toutefois, le risque d'invalidation est important, particulièrement à l'égard de l'utilisation des données à caractère personnel de citoyens européens par les autorités de surveillance américaines.

I. Traitement des données par l'Agence nationale de sécurité

A. Contextualisation

L'ampleur de l'évolution de la protection de données ne serait telle que sans les révélations de Edward Snowden[6]. En 2013, cet ancien employé de l'Agence nationale de sécurité (NSA) a mis en lumière la magnitude de l'écoute de masse sur Internet et des programmes de surveillance conduits par les États-Unis[7]. Dix ans plus tard, le DPF tente de mettre à niveau la protection des données relativement à son usage par la NSA à des fins de sécurité nationale[8].

B. Éclairage sur la législation américaine

Afin de saisir la portée du traitement des données personnelles par la NSA, il convient d'examiner les divers instruments juridiques qui le régulent. Le *Foreign Intelligence Surveillance Act* (FISA), dans sa Section 702, prescrit les activités de surveillance sur le territoire américain. Le décret présidentiel (EO) 14086 prévoit l'exécution de ces activités. À noter que le FISA est une loi issue du pouvoir législatif alors que le décret est une directive interne de l'exécutif et n'est pas opposable[9].

---

[1] CJUE, arrêt du 6.10.2015, *Schrems I*, C-362/14.

[2] CJUE, arrêt du 16.07.2020, *Schrems II*, C-311/18.

[3] S. Shackelford, Seeking a Safe Harbor in a Widening Sea, Wm. & Mary Bill Rts. J. 2/2021, p. 320 s.

[4] C. Kuner, art. 45 RGPD, in : Kuner et al. (édit.), The EU General Data Protection Regulation (GDPR): A Commentary, 2020 Oxford (ci-après « Kuner, art. »).

[5] Commission européenne, Décisions d'adéquation, in : https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (consulté le 7.10.23).

[6] C. De Terwangne/C. Gayrel, Le RGPD et les transferts internationaux de données à caractère personnel, in : C. de Terwangne/K. Rosier (édit.), Le Règlement général sur la protection des données (RGPD/GDPR), Bruxelles 2018, p. 303.

[7] M. Burri, Cross-border data flows and privacy in global trade law, OREP 1/2023, p. 91.

[8] Kuner (n. 4), art. 45 RGPD N 2.

[9] H. Ruschmeier, Nothing new in the west? The executive order on US surveillance activities and the GDPR, 14.11.22, in:

L'EO 14086 a été adopté en octobre 2022 dans le cadre de la négociation du DPF. Son objectif est de rendre conforme la législation interne aux exigences européennes. Pour ce faire, le cadre des activités de surveillance est solidifié par l'intégration de nouvelles garanties, telles que la collection de donnée proportionnée[10].

Concernant la mise en œuvre, le système repose sur la soumission annuelle, par le Procureur général et le Directeur du renseignement national, de certifications autorisant les programmes de surveillance prévus dans la Section 702, par la *Foreign Intelligence Surveillance Court* (FISC)[11]. Une fois les certifications approuvées, les agences peuvent légalement collecter les données[12].

II. Adéquation du niveau de protection

A. Les aspects litigieux

L'adéquation du niveau américain de protection des données avec le fonctionnement du droit européen susmentionné est hésitante (art. 45 RGPD). Par conséquent, il convient d'examiner les critères de la qualité de la base légale et de la proportionnalité à la lumière de la grille d'analyse élaborée par le Comité européen de la protection des données. Toutefois, il sied de mentionner les deux autres critères qui ne seront pas examinés : la *compliance* par des autorités indépendantes et le droit au recours effectif[13].

B. La précision des bases légales

En collectant les données de citoyens européens, les agences américaines peuvent porter atteinte à leurs droits fondamentaux (art. 7, 8 et 47 Charte des droits fondamentaux de l'UE)[14]. De ce fait, ces atteintes doivent se baser sur des règles claires, précises, accessibles et prévisibles pour être légitimes[15].

Cette condition n'impose pas que le fondement soit une loi formelle : il doit s'agir d'un acte contraignant en droit interne, sans nécessairement qu'il s'agisse d'un acte juridique issu du Parlement (*i.e.* Congrès)[16]. En outre, ce fondement doit démontrer une densité normative suffisante, déterminable à l'aide des critères suivants : définition des catégories de personnes susceptibles de faire l'objet d'une surveillance, limitation de la durée d'exécution et de conservation des données et précautions pour les transferts ultérieurs[17]. Bien que cela soit délicat dans le domaine de la surveillance, qui se veut secrète, une clarté sur la prévisibilité doit ressortir des règlementations[18].

L'EO 14086 définit explicitement les objectifs qui justifient une surveillance[19]. À cet égard, trois problèmes sont à soulever. Premièrement, les douze objectifs listés dans le décret sont si larges et vagues qu'il est difficile d'imaginer une raison qui ne pourrait trouver sa place dans l'une des catégories[20]. Il est douteux que cela puisse satisfaire les exigences de clarté normative. Deuxièmement, la liste démontre une différence entre les notions européenne et américaine de sécurité nationale. À titre d'exemple, les kidnappings du personnel d'État figurent sur la liste alors que la jurisprudence de la CJUE ne le qualifie pas comme une menace à la sécurité nationale[21]. Troisièmement, le cercle de ces raisons légitimes peut être élargi si le Président le juge nécessaire, sans même informer le public de ce changement[22].

Une pratique d'obtention de renseignement est particulièrement controversée : la collecte de masse

https://europeanlawblog.eu/2022/11/14/nothing-new-in-the-west-the-executive-order-on-us-surveillance-activities-and-the-gdpr/ (consulté le 10.11.23).

[10] Executive Order "Enhancing Safeguards for United States Signals Intelligence Activities" (EO 14086) du 7 octobre 2022, section II.

[11] A. Savin, The New Framework for Transatlantic Data Transfers, CBS Law 1/2023, p. 11.

[12] F. G'sell, *What will happen to transatlantic data transfers following the sanction imposed by the Irish dpc on meta?* 10.06.23, in : https://www.sciencespo.fr/public/chaire-numerique/en/2023/06/10/meta-fine-data-transfers/#:~:text=-Consequently%2C%20Meta%20is%20given%20a,decision%20was%20foreseeable%20and%20expected (consulté le 11.11.23).

[13] EDPB, Recommandation 02/2020 sur les garanties essentielles européennes pour les mesures de surveillance du 10 novembre 2020 (ci-après « EEGs ») N 24.

[14] EUR-LEX : 2012/C 326/02.

[15] EEGs (n. 13), N 28 ss.

[16] CJUE, arrêt du 6.10.2020, *Privacy International*, C-623/17, pt 68.

[17] CourEDH, arrêt *Weber et Saravia c. Allemagne* du 29.6.2006, requête n° 52934/00, §95.

[18] CourEDH, arrêt *Malone c. UK* du 2.8.1984, requête n° 8691/79, §65 s.

[19] EO 14086 (n. 10), Section II b.

[20] D. Korff, The inadequacy of the October 2022 new US Presidential Executive Order on Enhancing Safeguards For United States Signals Intelligence Activities, Oxford 2022, p. 8.

[21] *Idem*, p. 13.

[22] EO 14086 (n. 10), Section I b(i)(B).

(*bulk collection*)[23]. Tout d'abord, l'existence de cette pratique est remise en cause[24]. Ensuite, les garanties qui l'accompagnent sont vagues. Bien que le texte de l'EO 14086 précise qu'une *target collection* est préférable à une *bulk collection*[25], la manière d'appréhender cette subsidiarité est floue[26]. Certes, la *bulk collection* est limitée à la poursuite de seulement six objectifs, mais leur formulation est imprécise[27]. Par conséquent, un nombre exorbitant de personnes pourraient être ciblées sans qu'elles aient de lien direct avec la sécurité nationale[28]. Outre les imprécisions de formulation, une lacune dans le champ d'application matériel du décret est inquiétante : les données obtenues autrement que par la collecte par les autorités publiques ne sont pas couvertes, par exemple via l'achat de données à des *brokers* ou par leur obtention sur la base du *Cloud Act*[29].

C. La proportionnalité au sens large

S'il est admis que la fin poursuivie est la sécurité nationale, encore faut-il que la surveillance soit nécessaire et proportionnée, comme le prévoit désormais explicitement l'EO 14086[30]. Or, la proportionnalité a autant de définitions que de contextes juridiques dans lesquels elle s'imbrique. Les différentes compréhensions entraînent des conséquences tangibles, comme le révèle la comparaison entre le test de proportionnalité européen et américain.

1. La proportionnalité au sens strict

La pesée des intérêts entre la protection des données et la sécurité nationale diffère de part et d'autre de l'Atlantique, à un tel point que la proportionnalité, centrale dans la doctrine européenne, n'était pas une exigence dans les deux décisions d'adéquation précédentes[31]. La limitation de l'ingérence dans la vie privée n'étant pas prévue pour les citoyens non-américains, l'essence de ce droit fondamental était systématiquement violée[32]. Désormais, l'exigence de la proportionnalité est formellement inscrite. Cependant, les préoccupations persistent quant à l'interprétation américaine de cette notion[33]. L'EO 14086 explicite la proportionnalité en exigeant une « *proper balance* » et une « *collection as tailored as feasible* »[34]. En dépit de ces améliorations, il subsiste des doutes quant à la capacité de cette approche à contrer efficacement une pratique de *bulk collection*, par nature indiscriminée. À moins que les autorités américaines ne s'appuient sur la jurisprudence européenne et de droit international public, la mention de la proportionnalité dans le droit interne ne sera guère plus que du « *legal window dressing* »[35].

2. La nécessité

Le droit européen exige que les mesures de surveillance n'aillent pas au-delà du strict nécessaire, sans quoi elles seraient inadmissibles dans une société démocratique[36]. Afin de préserver les moyens de protection de leur sécurité nationale, les autorités américaines se réservent la liberté d'employer les mesures les plus efficaces[37]. Cela signifie que si la surveillance massive est adéquate pour une menace déterminée, il n'est pas requis que ce soit le seul moyen à disposition[38]. Selon toutes les indications, cette condition ne semble pas satisfaire pleinement les critères de nécessité rigoureuse tels qu'interprétés par la jurisprudence de l'UE[39].

Selon la doctrine européenne, la mesure doit être à même d'atteindre l'objectif, mais pas au-delà, à l'image d'une flèche qui vise à toucher une cible[40]. L'approche européenne privilégie une flèche de précision avec la puissance adaptée au but poursuivi. Outre-Atlantique, en revanche, si de nombreux arcs sont armés, cela

[23] B. Juliussen et al., The third country problem under the GDPR: enhancing protection of data transfers with technology, in : IDPL 3/2023, p. 229.
[24] *Ibidem*.
[25] EO 14086, Section II c(ii)(A).
[26] L. Drechsler et al., Third time is the charm?, in : CiTiP Working Paper 2023, p. 16 ss.
[27] Korff (n. 20), p. 12.
[28] Ruschmeier (n. 9).
[29] Z. Chabus, Where the fourth Amendment fails, in : U. Pitt. L. Rev. Online 5/2023, p. 9 s.
[30] EO 14086 (n. 10), Section II a(ii)(B).
[31] CJUE, arrêt du 16.7.2020, *Schrems II*, C-392/14, pts 168-185.
[32] K. Lenaerts, Limits on Limitations: The Essence of Fundamental Rights in the EU, GLJ 6/2019, p. 781.
[33] Juliussen et al. (n. 23), p. 231.
[34] EO 14086 (n. 10), Section II.
[35] Korff (n. 20), p. 12.
[36] EEGs (n. 13), N 22.
[37] Savin (n. 11), p. 7.
[38] *Ibidem*.
[39] Juliussen et al. (n. 23), p. 230.
[40] Savin (n. 11), p. 7.

répond à une nécessité aussi longtemps que les flèches sont orientées vers la cible. De cette illustration nous pouvons constater qu'un même état de fait sera justifié sous le régime américain et illégal sous l'européen. La doctrine européenne voit une violation du principe de nécessité lorsqu'il y a un accès généralisé ou que le rapport entre les données conservées et l'objectif poursuivi n'est pas donné, alors que la doctrine américaine valide de telles pratiques[41].

Conclusion

Au terme de notre étude, deux constatations se dégagent : un bilan normatif est inévitablement superficiel tandis qu'un bilan pragmatique est inévitablement pessimiste.

L'indispensabilité d'instruments juridiques robustes et contraignants est incontestable pour satisfaire aux exigences du RGPD. En revanche, le texte américain ne suffit pas à satisfaire aux standards européens. Partant, s'arrêter aux défauts prescriptifs du DPF ne nous semble pas opportun. Du moins, il ne serait pas souhaitable que la CJUE condamne le DPF de ce point de vue. La Haute Cour européenne se doit d'être intransigeante quant à la mise en pratique et son attention ne devrait être détournée par des préoccupations d'ordre normatif. Si, toutefois, elle devait considérer le DPF comme insatisfaisant, par souci de cohérence, il lui incomberait de se pencher également sur les décisions d'adéquation conclues avec Israël et le Japon, tous deux disposant de pratiques de surveillances similaires aux États-Unis[42]. Cela nous amène à mettre en lumière les doubles standards de l'Union entre ce qui est attendu par ses États membres et les États tiers[43]. Il est difficile de justifier les restrictions aux transferts de données vers un pays tiers en raison de ses lois sur la surveillance quand ces mêmes données peuvent librement circuler vers des États qui n'offrent pas plus de garanties à ce niveau, voire moins[44].

En ce qui concerne les perspectives du DPF, le 6 septembre 2023 a marqué le dépôt de la première demande en annulation du DPF auprès de la CJUE[45], et l'étape III de l'épopée *Schrems*, ainsi nommée en référence à l'avocat activiste qui a fait annuler le *Safe Harbor* et le *Privacy Shield*, ne devrait pas tarder à connaître un nouveau rebondissement.

[41] Juliussen et al. (n. 23), p. 232.
[42] *Ibidem*.
[43] Shackelford (n. 3), p. 326.
[44] Korff (n. 20), p. 28.
[45] P. Navarro/J. Schwartz, Member of French Parliament lodges first request for annulment of EU-US Data Privacy Framework, 8.9.23, in: *https://www.engage.hoganlovells.com/knowledgeservices/news/member-of-french-parliament-lodges-first-request-for-annulment-of-eu-us-data-privacy-framework* (consulté le 6.10.2023).