Réponse à l’appel à contribution préalable au rapport relatif au premier examen du DPF

6 septembre 2024

Table des matières

I] Sur la procédure de contribution

Il est inacceptable que cet appel à contribution se déroule durant le mois d'août et la rentrée, période sur laquelle la société civile et les personnes concernées (au sens du RGPD) se détendent, sont moins disponibles, etc. (Pour illustration : sur le mois d'août, la DG JUST a été incapable de me communiquer, dans les temps, le résultat de l'évaluation préliminaire de ma plainte pour manquement au droit de l'UE et le CEPD a été incapable de répondre à une demande d'information au sens du Règlement 1049/2001. Dès lors, comment espérer une plus grande disponibilité de simples citoyens et d'autres parties prenantes ?) Cela fait naître un doute malsain que la Commission européenne cherche à soustraire cet appel à contribution au regard des citoyens européens et autres parties prenantes. J'invite la Commission à ne pas organiser d'appel à contribution durant les périodes de repos communément admises (période estivale, période hivernale, etc.).

À titre subsidiaire, je constate que, par application de l'article 97 du RGPD, l'appel à contribution préalable au rapport d'évaluation 2024 du RGPD (https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14054-Rapport-sur-le-reglement-general-sur-la-protection-des-donnees_fr) portait sur le chapitre V du RGPD. Dès lors, je m'étonne de ce deuxième appel à contribution. Même si je le comprends (séparer les sujets pour plus de clarté), cela participe à l'épuisement des parties prenantes, notamment des citoyens, qui ont d'autres occupations que de répondre sans cesse à des appels à contribution, laissant ainsi le champ libre aux lobbyistes, payés pour ce faire, et biaisant de facto le résultat des appels à contribution, avec un préjudice sur la confiance accordée, par les citoyens, aux processus décisionnels de l'UE.

Le premier examen du DPF « vise à déterminer si tous les éléments du cadre sont en place et fonctionnent comme prévu ». Je comprends que la Commission souhaite interroger les parties-prenantes pour, précisément, déterminer l'effectivité et le bon fonctionnement du DPF. Néanmoins, il aurait été pertinent que la Commission alimente le présent appel à contribution avec des informations et documents permettant une analyse et une réflexion de fond : la Commission a-t-elle conduit et/ou poursuivie les négociations auxquelles l'invitait le Parlement européen dans sa résolution 2023/2501 du 11 mai 2023 ? Quel en a été le résultat ? Quel a été le résultat préliminaire des palabres européano-états-uniennes des 18 et 19 juillet 2024 ? Etc. L'appel à contribution se limite à énumérer les prétendus apports du DPF (notions de nécessité et de proportionnalité de la collecte états-unienne, Cour chargée du contrôle de la protection des données, obligations supervisées par la Commission fédérale du commerce, etc.) sans les nuancer ni énumérer d'éventuelles améliorations apportées suite aux critiques des parlementaires européens et de la société civile. En ne communiquant pas les informations et documents sus-mentionnés, la Commission ne met pas les parties prenantes, et notamment les citoyens, en capacité de participer utilement au présent appel à contribution, ne les rend pas actifs dans le processus décisionnel de l'UE. C'est fort dommage.

II] De la souveraineté européenne

Par « souveraineté », je laisse à d'autres le repli identitaire et j'entends un rapport de force entre puissances économiques mondiales, une maîtrise du risque en cas de défaut ou de contentieux avec un prétendu « allié », une indépendance en matière d'infrastructures et de services numériques, et le développement d'un marché et de filières économiques européens donc innovation, création de valeur économique, d'emplois, etc. au sein de l'UE.

Par conception, le RGPD a un objectif, un effet et un rôle de protectionnisme réglementaire (tout service irrespectueux de la vie privée peut-être évincé de l'espace économique européen) qui a tout son sens à l'heure des infrastructures numériques, des services numériques et de l'économie de la donnée. Ce protectionnisme est une opportunité de développer et de favoriser le business au sein de l'Union, donc l'innovation, l'emploi, la puissance économique et géopolitique, la croissance économique, etc. Il permet de développer des alternatives et de nouvelles infrastructures et services. Il permet de créer et de faire vivre toute une économie sur un fort respect de la vie privée : la protection des droits humains bénéficie à l'économie, en somme.

Pour que cela se concrétise, il est impératif de veiller à une stricte et rigoureuse application du RGPD, tant au sein de chaque État-membre de l'Union qu'en dehors, ce qui suppose de ne pas permettre la libre circulation des données à caractère personnel (DCP) avec des moins-disants, c'est-à-dire avec des cultures, des législations et des pratiques défaillantes en matière de respect de la vie privée, telles que celles des États-Unis d'Amérique (j'y reviendrai). Le DPF est un renoncement.

L'UE ne pourra pas être une puissance économique du numérique et toutes les autres promesses dont nous abreuve régulièrement la Commission européenne sans le versant protectionnisme du RGPD. L'UE ne pourra pas être une puissance économique du numérique en amoindrissant les droits humains, via le DPF, afin de confier nos DCP à des sociétés commerciales états-uniennes prédatrices et hégémoniques.

Sur le plan géopolitique, la décision d'adéquation du DPF a été adoptée quelques mois avant que le Congrès états-unien ait à se prononcer sur le renouvellement de la section 702 du FISA. En transigeant avec le DPF, l'UE s'est ainsi privée d'un levier de négociation par le biais de la taille de son marché économique. Il s'agit d'une faute lourde imputable à la Commission européenne.

Je rappelle que les États-Unis d'Amérique n'hésitent pas à pratiquer, eux, un protectionnisme réglementaire, y compris en matière de numérique et de données à caractère personnel. Voir : https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/ ou encore le Protecting Americans from Foreign Adversary Controlled Applications Act.

Il est temps que l'UE sorte de sa naïveté et de l'emprise états-unienne. Or, le DPF ne va pas dans le sens d'une émancipation.

III] Validité du DPF au regard de la Charte des droits fondamentaux

La validité du DPF au regard du droit européen et sa compatibilité avec la protection de la vie privée, des libertés et des droits fondamentaux des personnes concernées pose question. Le Comité européen de la protection des données (CEPD), le Parlement européen, et l'ONG NOYB (dont le président est le requérant à l'origine des arrêts de la CJUE invalidant les précédentes décisions d'adéquation avec les États-Unis d'Amérique) se sont montrés mitigés voire sceptiques sur les apports et la conformité au droit de l'Union du décret présidentiel états-unien EO 14086 et du DPF. Voir : https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_en, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_FR.html, et https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu.

En effet, plusieurs éléments ayant conduit à l'invalidation des précédentes décisions d'adéquation (Safe Harbor dans C-362/14, Privacy Shield dans C-311/18) demeurent inchangés :

- Les États-Unis d'Amérique ne disposent pas d'une loi fédérale ni d'une culture de la protection de la vie privée. La conception européenne des données à caractère personnel (DCP) comme étant des émanations d'une personne physique, encadrées par des droits incessibles, est remplacée par la *privacy*, c'est-à-dire une conception patrimoniale dans laquelle les DCP sont des propriétés cessibles et où la démonstration d'une atteinte portée à ces données ne se conduit pas de la même manière (atteinte à une personne versus préjudice économique) ;

- La réglementation fédérale états-unienne et les programmes de surveillance ayant conduit à l'invalidation des décisions d'adéquation précédentes (cf. C-311/18, paragraphes 178 à 180), notamment la section 702 de la loi Foreign Intelligence Surveillance Act (FISA), la loi Stored Communications Act (SCA) amendée par la loi Clarifying Lawful Overseas Use of Data Act (CLOUD Act), et les Executive Order 12333 (« United States Intelligence Activities ») et 14086 (« Enhancing Safeguards for United States Signals Intelligence Activities »), permettent toujours aux autorités publiques états-uniennes, notamment pour des motifs de sécurité nationale ou « d'intérêt public » qui prédominent sur le DPF (cf. l'annexe 1(I)(5) de la décision d'exécution 2023/1795 et le paragraphe 164 de l'arrêt C-311/18 de la CJUE), d'accéder, de manière généralisée et sans contrôle judiciaire ou administratif spécifique, indépendant et préalable, au contexte et au contenu des communications électroniques des Européens quand elles sont hébergées, traitées ou en transit par des entités états-uniennes. Je rappelle que le décret 14086 ne s'applique pas aux accès, par les autorités publiques états-uniennes, aux données collectées par les mécanismes du CLOUD Act, par ex. ;

- La collecte, le stockage, et l'accès indiscriminés aux communications électroniques qui résultent du point précédent sont dissimulés derrière un verbiage juridique (« nécessité », « proportionnalité », « collecte en vrac », etc.) imitant celui de la CJUE sans y être conforme en pratique : divergence sur la définition de ces termes (cf. la résolution du Parlement européen et l'avis de NOYB sus-pointés). Cette divergence, tant de culture que de tradition juridique, semble très difficilement soluble ;

- Le renseignement états-unien poursuit une liste d'objectifs qui peut varier dans le temps sans information obligatoire de l'UE (cf. section 2(b)(i)(B) de l'EO 14086). Ces objectifs, cette priorité en matière de renseignement, prévaut sur le DPF et sur les notions de nécessité et de proportionnalité de la collecte et du traitement des DCP ;

- Un recours par un Européen se forme toujours aux États-Unis, devant un comité dépendant in fine de l'exécutif états-unien (voir en ce sens https://www.edpb.europa.eu/system/files/2024-04/edpb_information-note_dpf-redress-mechanism-national-security-purposes_en.pdf – « the U.S. Department of Justice's Office of Privacy and Civil Liberties ('OPCL'), which provides support to the DPRC […] » – versus C-311/18, paragraphe 195) et créé par lui (et non par une loi), dont le pouvoir contraignant n'est pas garanti (voir C-311/18, paragraphe 196), qui répondra toujours une réponse-type qui ne pourra toujours pas faire l'objet d'un appel devant une véritable juridiction fédérale. De plus, avant de former un recours, encore faut-il être informé être sous surveillance… Pas simple, pour un Européen. La sécurité nationale états-unienne, c'est-à-dire in fine la raison d'État, annihile tout droit opposable et tout recours effectif ;

- Les entités états-uniennes importatrices de données continuent de s'auto-certifier conformes (en adéquation, offrant un même niveau de protection) au droit de l'UE auprès du Département du Commerce états-unien, en adhérant volontairement au DPF, sans contrôle indépendant. Plusieurs multinationales qui, pourtant, transfèrent des DCP vers les États-Unis d'Amérique n'ont pas renouvelé leurs agréments : Airbnb n'a jamais obtenu son agrément sous le DPF, idem pour Mailgun et Piano Software, et Twitter l'a perdu entre le 30 mars 2023 et le 4 avril 2024, par exemple. Absence de suivi dans le temps, donc. En pratique, le DPF est perçu, tant par les responsables de traitements (et DPO) exportateurs de données, que par les entités états-uniennes importatrices, comme un blanc-seing. Peu leur importe le contrôle de la sous-traitance (article 28 du RGPD), l'analyse de risque, les garanties techniques et organisationnelles (article 44 et suivants du RGPD), la sécurité du transfert (article 32 RGPD), etc. Des entités états-uniennes prospérant sur un modèle économique incompatible avec le RGPD et/ou déjà sanctionnées à de multiples reprises par des autorités de contrôle européennes (article 51 et suivants du RGPD) sont « labelisées » DPF… Bref, le mot d'ordre est « faisons n'importe quoi, la circulation des DCP est libre, DPF, tout ça ». L'autorité de contrôle française, la CNIL, clôture toute réclamation visant des transferts hors UE au motif qu'ils sont couverts par le DPF sans s'interroger sur la validité juridique de celui-ci (C-311/18, paragraphes 119 à 120 et 156 à 158) ni sur la conformité réelle et effective du traitement / transfert, tant du côté de l'exportateur européen que de l'importateur états-unien ;

- Les exceptions au cadre, permises par celui-ci, sont floues.

Dans son avis 5/2023 sus-pointé, le CEPD expose que les principes du DPF sont essentiellement les mêmes que ceux du Privacy Shield (page 3), et que les voies de recours sont identiques (page 4). Dès lors, le DPF n'est pas plus conforme à l'article 45(2)(a) du RGPD et à la Charte des droits fondamentaux de l'UE que ne l'était le Privacy Shield.

Il ressort de tout ce qui précède qu'il existe un doute sérieux que les États-Unis ne proposent pas un niveau élevé de protection des données à caractère personnel et des droits (cf. considérant 10 du RGPD et CJUE, C-26/22 et C-64/22, paragraphe 61), et, ce

faisant, que la décision de la Commission européenne constatant un niveau de protection en adéquation avec celui de l'UE soit invalide.

Le 20/04/2024, le président états-unien a promulgué la loi Reforming Intelligence and Securing America Act (RISAA, https://www.congress.gov/bill/118th-congress/house-bill/7888/text/enr, https://arstechnica.com/tech-policy/2024/04/biden-signs-bill-criticized-as-major-expansion-of-warrantless-surveillance/). Celle-ci, entre autres :

- Prolonge, entre autres, la loi FISA pour deux ans, y compris donc les programmes de surveillance fondés sur sa section 702 qui ont conduit à l'invalidation du Privacy Shield (C-311/18, paragraphes 178 à 180) ;

- Étend la définition de « fournisseur de services de communications électroniques » sommé de collaborer avec le renseignement états-unien pour englober tout prestataire de service qui a accès à un équipement utilisé pour transmettre ou stocker des communications électroniques (moyennant une exception pour les hôtels, les restaurants, les habitations, etc.), ce qui pourrait inclure, par exemple, les exploitants de centres de données (datacenters). Avant, la loi visait uniquement les opérateurs de télécommunications, les fournisseurs de services de communication électronique, les fournisseurs de services informatiques à distance et tout fournisseur de services de communication qui a accès à des communications électroniques lors de leur transmission ou de leur stockage. Durant les débats parlementaires, l'Information Technology Industry Council, le lobby des multinationales états-uniennes du numérique, déclarait (https://www.itic.org/news-events/techwonk-blog/expansion-of-fisa-electronic-communications-service-provider-definition-must-be-removed): « Beyond the immediate impacts of sweeping a multitude of additional entities within FISA 702's scope, we should also consider the wider impacts on the competitiveness of U.S. technology companies and, potentially, trusted data flows with U.S. allies. […] just last year, as part of implementing its commitments pursuant to the new EU-U.S. Data Privacy Framework, President Biden issued Executive Order 14086, […], enabling the continued free flow of data across the Atlantic. It would be a step backwards to embrace an amendment that now, less than a year later, would greatly expand the scope of a key foreign surveillance authority » ;

- Exacerbe la distinction entre les citoyens états-uniens, à qui elle prétend garantir toujours plus la protection de leur vie privée et de leurs libertés, et les autres, qui continueront à faire l'objet de la surveillance. Je cite https://arstechnica.com/tech-policy/2024/04/biden-signs-bill-criticized-as-major-expansion-of-warrantless-surveillance/ : « US Attorney General Merrick Garland praised the FISA reauthorization, saying it gives the US "authority to continue to collect foreign intelligence information about non-US persons located outside the United States, while at the same time codifying important reforms the Justice Department has adopted to ensure the protection of Americans' privacy and civil liberties." »

Des amendements ont proposé de retirer l'obligation d'obtention d'un mandat préalablement à la surveillance d'un citoyen états-unien ou bien encore d'étendre la section 702 de la loi FISA aux visiteurs, demandeurs d'asile et résidents permanents (https://arstechnica.com/tech-policy/2023/12/green-card-applicants-targeted-by-section-702-foreign-intelligence-bill/). Cela démontre une tension, une pression, une volonté d'étendre la surveillance étatique.

Indépendamment de la loi RISAA mais en simultané, le directeur adjoint du FBI a invité ses troupes à faire un usage fréquent de la surveillance sans mandat des citoyens

états-uniens afin d'être en capacité de justifier l'utilisation du dispositif et donc son maintien (https://arstechnica.com/tech-policy/2024/05/fbi-urges-employees-to-look-for-ways-to-collect-americans-messages/). Il est donc bien question d'un usage superflu et disproportionné en cela qu'il n'est pas justifié par un besoin réel de sécurité nationale ou « d'intérêt public ».

Cette invitation, la loi RISAA, et le débat parlementaire attenant, font douter du sérieux des engagements pris par les États-Unis lors de la négociation du DPF et de l'effectivité des garanties incluses dans l'EO 14086. Au contraire, elles confortent l'analyse d'une réglementation toujours renforcée, de pratiques de surveillance persistantes, d'une culture et d'une conception des données à caractère personnel qui ne sont pas conformes au droit de l'UE.

Étant donné :

- la conception divergente, entre les États-Unis d'Amérique et l'UE, de la vie privée, de la nature profonde des données à caractère personnel, et des notions de « nécessité » et de « proportionnalité » des ingérences dans les droits fondamentaux ;

- la discrimination constitutionnelle dans l'octroi de droits et de protection contre les ingérences étatiques entre les citoyens états-uniens (US person) et le reste du monde pratiquée par les États-Unis d'Amérique ;

- l'auto-certification sans contrôle et bidonnée (décorrélée de la réalité, de leurs pratiques techniques et organisationnelles effectives), par les entités états-uniennes importatrices de données à caractère personnel d'Européens, de leur adéquation avec le droit de l'UE ;

- l'existence légale, réelle et documentée d'une surveillance massive, indiscriminée, sans contrôle préalable, et au-delà de toute nécessité et proportionnalité, des communications électroniques des Européens quand elles sont hébergées, traitées ou en transit via des entités états-uniennes, par les autorités publiques états-uniennes, notamment pour des motifs de sécurité nationale et d'intérêt public qui prédominent sur les accords internationaux dont les décisions d'adéquation de l'UE ;

- l'absence de droits opposables visant à prévenir l'accès aux données à caractère personnel d'un Européen et à lui octroyer la communication, la rectification, et la suppression desdites données ou la limitation de leur traitement ;

- et l'absence de recours effectif auprès d'une juridiction indépendante et contraignante dans le cadre d'un procès équitable,

le DPF semble méconnaître les articles 7, 8, 47 ou 52(1) de la Charte des droits fondamentaux de l'UE ainsi que les articles 45(1) ou 45(2) du RGPD.

IV] Conclusion

Le droit états-unien est profondément incompatible avec le droit européen. Il s'agit de divergences culturelles, de tradition juridique, et constitutionnelles. Dès lors, un accord international tel le DPF ne saurait suffire.

Le DPF nuit aux droits fondamentaux des Européens ainsi qu'au développement de l'économie numérique européenne en amoindrissant considérablement l'effet protectionniste du RGPD.

En conséquence, le DPF doit être abrogé et l'économie numérique européenne, notamment celle en matière d'infrastructures et de services numériques, en sus d'être lourdement contrôlée par les autorités de contrôle (article 51 et suivants du RGPD), doit être soutenue par le développement de filières par, entre autres, des investissements massifs, y compris dans la formation, le fléchage de la commande publique, le subventionnement, la mutualisation par l'offre ou par la demande sous l'impulsion publique, etc. visant à créer des débouchées, etc. Ainsi, nous parviendrons à être une puissance économique très respectueuse de la vie privée des citoyens.