Etat des lieux suite au décret exécutif américain sur le transfert des données personnelles UE-USA

Par Florian de VAULX

Gérant de la société Datasure
Ingénieur informatique diplômé du Conservatoire national des arts et métiers (Cnam)
Doctorant au Centre d'études internationales de la propriété intellectuelle (CEIPI)
Université de Strasbourg

➔RLDI 4583

Ce mois d'octobre, déclaré mois de la cybersécurité par l'ANSSI, ne manquait pas d'actualités à commenter et l'une d'elles était particulièrement attendue : la signature d'un décret exécutif par le président Biden le 7 octobre 2022[1] afin d'avancer, enfin, sur la question majeure du transfert des données personnelles entre l'Union européenne et les Etats-Unis.

Après plus de deux ans d'incertitudes juridiques, cette nouvelle vient rassurer les centaines de milliers d'entreprises qui transfèrent chaque jour des données personnelles de l'UE vers les Etats-Unis. Une nouvelle voie semble donc se dessiner dans le brouillard d'insécurité juridique qu'avait alors instauré l'arrêt dit « Shrems II » de la Cour de Justice de l'Union européenne (CJUE)[2], en invalidant le principal instrument juridique servant de fondement à ces transferts conformément à l'article 45 du Règlement général sur la protection des données (RGPD)[3].

Dès l'annonce de signature du décret exécutif américain, la Commission européenne se félicitait le même jour de pouvoir ainsi démarrer le processus de rédaction et d'adoption de la nouvelle décision d'adéquation[4]. Ce troisième texte, après l'invalidation coup sur coup par la CJUE du « *Safe Harbor* » en 2015 puis du « *Privacy Shield* » en 2020, est né d'un accord entre Joe Biden et Ursula von der Leyen en mars dernier[5]. La simultanéité de cet arrangement avec la question de la fourniture d'énergies par les américains au profit de l'Europe n'avait d'ailleurs pas manqué de faire réagir certains commentateurs.

ETATS-UNIS : « UN PARTENAIRE À GÉOMÉTRIE VARIABLE »

Dans le même temps en France, l'avant-veille du décret Biden, la Commission des affaires étrangères et de la défense du Sénat auditionnaient Stéphane Bouillon, Secrétaire Général du Secrétariat général de la Défense et de la Sécurité nationale (SGDSN) et Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)[6]. Sur la question posée par la Commission de savoir si les Etats-Unis étaient un « *partenaire à géométrie variable selon que l'on parle de cyber, de sous-marin ou de visites d'Etat* », Stéphane Bouillon a rappelé que les relations entre les deux puissances étaient indispensables et de qualité, non sans conclure par une recommandation à la vigilance par la maxime : « *un Etat n'a pas d'amis, mais que des intérêts* ».

Il faut dire que le rapport de force entretenu par les Etats-Unis vis-à-vis de l'Europe et, en particulier de la France, est parfois qualifié de « *guerre économique* » comme l'illustre des dossiers très sensibles tels que ceux d'Alstom ou d'Airbus. Le recours à des lois extraterritoriales américaines renouvelle sans cesse le débat sur la souveraineté française ou européenne, ainsi que sur notre capacité à protéger nos entreprises et nos données, particulièrement à cet

(1) White House, 7 octobre 2022, *FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework, Consulté en ligne [https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/]*

(2) CJUE, gd. Ch., 16 juill. 2020, aff. C-311/8, Facebook Ireland et Schrems.

(3) 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. général sur la protection des données)

(4) *European Commission, Questions & Answers : EU-U.S. Data Privacy Frameworkn* https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_6045

(5) Commission européenne, 25 mars 2022, Déclaration de la Présidente Von der Leyen avec le Président Biden. Communiqué de presse, https://ec.europa.eu/commission/presscorner/detail/fr/STATEMENT_22_2043

(6) Commission des affaires étrangères, de la défense et des forces armées, 5 octobre 2022, PLF 2023 - Audition de MM. Stéphane Bouillon (SGDSN) de Guillaume Poupard (ANSSI) http://videos.senat.fr/video.3008437_633b624b3e4ca.plf-2023---audition-de-mm-stephane-bouillon-sgdsn-de-guillaume-poupard-anssi-et-de-de-m-emmanu

instant où la guerre frappe en Europe suite à l'invasion de l'Ukraine par la Russie.

Olivier de Maison Rouge, spécialiste du droit de l'intelligence économique, rappelle que le concept de « *sécurité nationale* » aux Etats-Unis diffère substantiellement de l'approche historique française et leur permet de « *dépasser largement le seul cadre de la défense militaire et des armées.* »[7] , pour y inclure des considérations bien plus larges, telle que la bonne marche de leur économie nationale.

Il est aussi certain que les révélations d'Edward Snowden ont permis aux européens de sortir d'une forme de naïveté quant à la captation de leurs données par les services de renseignements américain.

Pour le numéro 1 de l'ANSSI, Guillaume Poupard, nul doute donc que le nouvel accord trouvé aura vocation à être annulé « d'ici à 4 ans » si les règles de bases ne sont pas changées[8]. Il faut dire que l'arsenal juridique à portée extraterritoriale des Etats-Unis est désormais bien connu[9], c'est précisément cela qui posait problème à la CJUE lors de l'arrêt « Shrems II ».

DES TRAITEMENTS DE DONNÉES PERSONNELLES ILLÉGAUX DEPUIS « SHREMS II »

Depuis l'arrêt de 2020 de la CJUE, le transfert de données à caractère personnel de citoyens européens vers les Etats-Unis est par principe considéré comme contraires à la Charte des droits fondamentaux de l'Union européenne en ce que la surveillance américaine sur ces données personnelles serait excessive, insuffisamment encadrée et surtout, n'admet pas la possibilité d'un recours effectif par les personnes concernées.

Dans un mémoire déposé par la CNIL à la demande du Conseil d'Etat au sujet du recours à Microsoft dans le dossier brûlant du Health Data Hub, l'autorité indépendante rappelle que le constat d'illégalité consécutif à la décision de la CJUE concerne aussi bien les données transférées que celles hébergées directement en Europe par une société américaine : la société mère étant de droit américain, elle reste soumise aux lois américaines. A la demande des services de renseignement américains, elle pourrait être contrainte de communiquer les données concernées, y compris si celles-ci sont hébergées en France[10].

Cette dernière considération semble conclure à l'illégalité d'à peu près tous les traitements de données à caractère personnel de l'économie européenne en raison de l'hégémonie des acteurs américains dans les solutions en *Cloud*. Ni les autorités nationales ni les institutions européennes ne semblent pourtant oser aussi clairement et publiquement l'affirmer, et pour cause : la conformité est en pratique très difficile, voire impossible à mettre en œuvre pour les acteurs économiques.

Il ressort en effet depuis l'arrêt « Shrems II » qu'un tel transfert doit être encadré par des garanties appropriées, plus précisément des « mesures complémentaires » qui tendent à compenser le fait que le droit des États-Unis n'assure pas un niveau de protection substantiellement équivalent à celui garanti par l'article 47 de la Charte.

En pratique, il s'agit d'empêcher les services de renseignement américains d'accéder en clair aux données personnelles des européens : le chiffrement de données ou l'anonymisation constituent ainsi des moyens sérieux envisageables pour apporter des garanties appropriées, rendues nécessaires en l'absence de décision d'adéquation. Problème : ces mesures sont très complexes à mettre en œuvre dans les différents contextes « métiers » actuels des organisations.

DES MESURES COMPLÉMENTAIRES DIFFICILES À METTRE EN ŒUVRE DANS LA PRATIQUE : L'EXEMPLE DU CHIFFREMENT

Le chiffrement est l'opération informatique par laquelle une donnée en clair devient inintelligible à ceux qui ne disposent pas de l'instrument pour la déchiffrer (nommé clé privée ou une clé secrète, selon le type de chiffrement dont il est question).

A l'ère du *cloud computing*, la question du chiffrement est complexe et, inévitablement, technique. Pour des solutions SaaS, le sujet central est de savoir qui détient la clé permettant de déchiffrer les données. En pratique, il est nécessaire pour le fournisseur de la solution de détenir cette clé afin de pouvoir servir les données « à la volée » pour l'utilisateur : ainsi, malgré toutes les garanties morales ou techniques affichées par ces fournisseurs américains, il n'empêche que si les données peuvent être déchiffrées par ces derniers à un instant *T*, elles pourront alors être captées par les services de renseignement américains.

C'est ainsi que les cas de réels chiffrements dans le *cloud* ne sont pour l'heure pas légion, mais le sujet étant directement lié à la nécessité de *compliance* des organisations, des initiatives voient régulièrement le jour dont on ne sait pas encore si elles iront réellement plus loin que les inefficiences précédemment constatées[11].

Pour certains, il faudrait reconnaître que la souveraineté absolue reste un vœu pieu en matière de numérique[12]. Les tenants de

(7) de Maison Rouge, O.. 28 juin 2019, Ecole de Pensée sur la Guerre économique (EPGE) https://www.epge.fr/guerre-economique-et-strategie-de-securite-nationale/

(8) *Cf. supra*

(9) Notamment *Cloud Act*, FISA (section 702) et *Executive Order (EO)* 12333.

(10) CNIL, 14 octobre 2020, « Le Conseil d'État demande au Health Data Hub des garanties supplémentaires pour limiter le risque de transfert vers les États-Unis », https://www.cnil.fr/fr/le-conseil-detat-demande-au-health-data-hub-des-garanties-supplementaires

(11) Citons ainsi l'exemple de l'éditeur N°1 mondial Salesforce, qui propose une option de chiffrement basé sur un système de cache temporaire, mais dont il possède temporairement la clé privée malgré les encapsulations techniques qui tentent de le faire oublier. Une annonce récente semble vouloir aller plus loin en y mêlant des gestionnaires extérieurs de clés tels qu'Atos et Thalès, pas sûr cependant que cela ne change grand-chose au constat précédent : peu importe qui génère et détient la clé de déchiffrement, dès lors qu'elle est nécessairement partagée au fournisseur de solution à un moment ou à un autre.

(12) *Cf. supra* Guillaume Poupard, audition devant la Commission des affaires étrangères, de la défense et des forces armées, 5 octobre 2022, PLF 2023 - Audition de MM. Stéphane Bouillon (SGDSN) de Guillaume Poupard (ANSSI).

cette souveraineté numérique « souple » considèrent ainsi qu'il peut être excessif de voir les fournisseurs de solutions américaines comme des ennemis et appellent plutôt au compromis technologique et juridique.

LE COMPROMIS TECHNOLOGIQUE ET JURIDIQUE, LA FAUSSE BONNE SOLUTION ?

En 2021, l'Etat français s'était montré favorable à un « cloud de confiance » mêlant les solutions logicielles américaines à une infrastructure sous seul pavillon français : le capital social devrait être majoritairement détenu par des français et donc, *a priori*, à l'abri des lois extraterritoriales américaines. Probablement à travers un système de licences complexe en termes de propriété intellectuelle, des américains tels que Microsoft, Google et Amazon devraient ainsi bientôt proposer leurs services numériques via des entreprises françaises telles que Orange et Capgemini (projet « Bleu »), Thalès (projet « S3ns ») ou encore Atos (non encore officiellement dévoilé).

Fausse bonne idée, d'après l'écosystème français qui prône une souveraineté numérique sans concession. Le député Philippe Latombe, rapporteur de la mission d'information *« Bâtir et promouvoir une souveraineté numérique nationale et européenne »*, avait ainsi donné son avis tranché sur le sujet en dénonçant à la CNIL, l'ANSSI, l'Autorité de la concurrence et la DGCCRF une « tentative d'enfumage » de certains des acteurs concernés.

Il persiste en effet, pour les tenants d'une souveraineté numérique française et européenne absolue, des risques importants de soumission aux lois extraterritoriales américaines malgré toutes les bonnes intentions affichées par les GAFAM.

VERS UN NOUVEL ARRÊT « SHREMS III » ?

Le 7 octobre dernier, la Maison Blanche annonçait que le nouvel accord EU-USA aura vocation à répondre aux préoccupations soulevées par la Cour de Justice de l'Union européenne.

Il est vrai que certains principes du RGPD font leur apparition dans le décret américain : le principe de minimisation[13], mais aussi des considérations relatives à la durée de conservation[14], à l'obligation de sécurité[15], au principe d'exactitude[16]…

Surtout, c'est la notion européenne de *« proportionnalité »* qui y est reprise, directement en lien avec les exigences de la Charte des droits fondamentaux de l'UE de nécessité et de proportionnalité quant aux limitations portées aux droits et libertés reconnues, tels que le droit au respect de la vie privée[17] ou à la protection des données à caractère personnel[18].

Est-ce pour autant suffisant ? Du côté de Max Shrems, via son association Noyb, on souligne que si les termes lexicaux utilisés sont désormais bien alignés en accord avec la Commission européenne, la signification juridique que les Etats-Unis donnent à la notion de proportionnalité pourrait différer substantiellement de l'interprétation de la CJUE. D'après Max Shrems : *« L'UE et les États-Unis sont désormais d'accord sur l'utilisation du mot «proportionné» mais semblent en désaccord sur sa signification. En fin de compte, c'est la définition de la CJUE qui prévaudra - ce qui risque de tuer à nouveau toute décision de l'UE. La Commission européenne ferme à nouveau les yeux sur la loi américaine, pour permettre de continuer à espionner les Européens. »*[19].

D'autres points majeurs semblent potentiellement mener à un futur contentieux devant la CJUE, comme par exemple le nouveau mécanisme de recours. Le décret met en place une *« Data Protection Review Court »* chargée de connaître des recours en la matière : difficulté majeure, il ne s'agira *a priori* pas d'un tribunal indépendant au sens de la Charte, mais d'une entité dépendant du pouvoir exécutif américain. Il est ainsi peu probable que la CJUE considère le recours à celle-ci comme un véritable « recours juridictionnel », ce qui était l'un des principaux motifs d'invalidation du Privacy Shield en 2020.

CONCLUSION

La Commission européenne doit désormais travailler sur la nouvelle décision d'adéquation conformément à l'article 45 du RGPD, et recueillir ensuite l'avis du Comité européen de protection des données (EDPB) et des pays membres. Le texte final n'est pas attendu avant le printemps 2023. Ce n'est qu'une fois celui-ci validé qu'il servira de fondement aux responsables de traitement pour le transfert de données personnelles UE-USA. En tout cas, jusqu'à ce qu'il fasse, certainement comme ses deux prédécesseurs, l'objet de recours devant les juridictions nationales et européennes… Gageons que nous n'en aurons pas fini de sitôt avec l'insécurité juridique en la matière. ■

(13) III, (A) *in Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities*, 7 octobre 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/

(14) III, (A), (2) (b) *Ibid*

(15) III, (B) *Ibid*

(16) III, (C) *Ibid*

(17) Article 7 de la Charte des droits fondamentaux de l'Union européenne

(18) Article 8 *Ibid*

(19) NOYB, 7 octobre 2022, «Première réaction : Le décret sur la surveillance américaine a peu de chances de satisfaire au droit européen »,https://noyb.eu/fr/le-nouveau-decret-americain-peu-de-chances-de-satisfaire-la-legislation-europeenne