Le transfert des donnÃ©es Ã caractÃ¨re personnel depuis lâ€™Europe vers les Ã‰tats-UnisÂ : oÃ¹ en est le projet de dÃ©cision dâ€™adÃ©quation de la Commission europÃ©enneÂ ?

Description

Alors que lâ€™on vient dâ€™apprendre que lâ€™autoritÃ© de contrÃ´le irlandaise a rendu une dÃ©cision historique en condamnant Meta Ã une amende administrative record de 1,2Â milliard dâ€™euros pour avoir rÃ©alisÃ© des transferts de donnÃ©es Ã caractÃ¨re personnel vers les Ã‰tats-Unis, en violation de lâ€™article 46 du RGPD, lâ€™Ã©tat dâ€™avancement du nouveau projet dâ€™adÃ©quation de la Commission europÃ©enne, dont lâ€™adoption permettrait de restaurer un libre transfert des donnÃ©es vers les entreprises amÃ©ricaines adhÃ©rant au cadre proposÃ©, est plus que jamais scrutÃ©Â ; or celui-ci ne paraÃ®t pas encore de nature Ã satisfaire les attentes europÃ©ennes.

1. Schrems IÂ â€“ Sous lâ€™impulsion du dÃ©sormais cÃ©lÃ¨bre Maximilien Schrems, la Cour de justice de lâ€™Union euroÂpÃ©enne (CJUE) a invalidÃ©, dans un arrÃªt du 6Â octobre 2015 communÃ©ment appelÃ©Â Â«Â Schrems IÂ Â»[1], la dÃ©cision dite dâ€™Â«Â adÃ©quationÂ Â»Â par laquelle la Commission europÃ©enne avait reconnu que le systÃ¨me dit Safe Harbor assurait un niveau de protectionÂ Â«Â adÃ©quatÂ Â»Â aux donnÃ©es qui Ã©taient transmises aux entreprises amÃ©ricaines y adhÃ©rant.
2. Schrems IIÂ â€“ Cette invalidation a conduit la Commission Ã renÃ©gocier avec les Ã‰tats-Unis un nouveau systÃ¨me baptisÃ© Privacy Shield, dont la Commission a reconnu le caractÃ¨re adÃ©quat par une seconde dÃ©cision dâ€™adÃ©quation qui fut elle aussi contestÃ©e, Ã lâ€™initiative de M.Â Schrems, et invalidÃ©e par la CJUE dans un arrÃªt du 16Â juillet 2020[2Â] immÃ©diatement baptisÃ©Â Â«Â SchremsÂ IIÂ Â».
3. Situation rÃ©sultanteâ€“ Cette seconde invalidation a obligÃ© les exportateurs europÃ©ens de donnÃ©es Ã fonder Ã nouveau leurs transferts de donnÃ©es vers les Ã‰tats-Unis sur lâ€™une des garanties Ã©noncÃ©es Ã lâ€™article 46 du rÃ¨glement gÃ©nÃ©ral sur la protection des donnÃ©es (RGPD) â€“ au premier chef les clauses contractuelles types adoptÃ©es par la Commission europÃ©enne â€“ ou encore sur lâ€™une des dÃ©rogations pour situation particuliÃ¨re prÃ©vues Ã lâ€™article 49 du rÃ¨glement.

Mais lâ€™autre apport de lâ€™arrÃªt Schrems II a rendu singuliÃ¨rement plus complexe le recours Ã ces alternativesÂ : il sâ€™agit de la nÃ©cessitÃ© de dÃ©terminer, en outre, si un risque existe que les autoritÃ©s publiques du pays de destination puissent intercepter les donnÃ©es et, dans lâ€™affirmative, dâ€™adopter des mesures supplÃ©mentaires de nature Ã neutraliser ce risque.

Il Ã©tait donc attendu de la Commission europÃ©enne quâ€™elle reprenne des nÃ©gociations avec les autoritÃ©s amÃ©ricaines en vue de lâ€™adoption dâ€™un nouveau programme pouvant bÃ©nÃ©ficier dâ€™une dÃ©cision dâ€™adÃ©quation.

4. Un nouveau projetÂ â€“ En mars 2022, la Commission a annoncÃ© avoir conclu avec les Ã‰tats-Unis un accord de principe quant Ã un projet deÂ Â«Â cadre transatlantique de protection des donnÃ©es personnellesÂ Â»Â ayant vocation Ã constituer lâ€™armature dâ€™un nouveau cadre juridique pour les transferts de donnÃ©es depuis lâ€™Europe vers les Ã‰tats-Unis. Cet accord de principe a dÃ©bouchÃ©, le 13Â dÃ©cembre 2022, sur la publication[3]Â dâ€™un projet de dÃ©cision dâ€™adÃ©quation dont les annexes constituent le nouveau Data Privacy Framework (DPF) devant sâ€™appliquer aux organisations amÃ©ricaines qui se seront autocertifiÃ©esÂ conformÃ©ment aux exigences posÃ©es par ce cadre.

En application de lâ€™article 70(1)(s) du RGPD, la Commission a requis sur ce projet de dÃ©cision lâ€™avis du ComitÃ© europÃ©en de la protection des donnÃ©es (CEPD), lequel a Ã©tÃ© rendu le 28Â fÃ©vrier 2023[4]. Dans quelle mesure la Commission a-t-elle rÃ©ussi Ã convaincre lâ€™expert europÃ©en de la protection des donnÃ©es Ã caracÂtÃ¨re personnel que son nouveau projet est adÃ©quatÂ ?

ProcÃ©dant Ã une analyse mÃ©thodique du nouveau cadre proposÃ©, le CEPD a relevÃ© des amÃ©liorations par rapport au systÃ¨me antÃ©rieur, mais aussi, et surtout, des interrogations et des points dâ€™inquiÃ©tude.

5. Les points de satisfactionÂ â€“ Au titre des amÃ©liorations, le CEPD relÃ¨ve que lâ€™*executive order(EO) 14086*[5], publiÃ© par le prÃ©sident amÃ©ricain en octobre 2022 et visant Ã remÃ©dier aux dÃ©fauts soulevÃ©s par la CJUE dans son arrÃªt Schrems II, constitue un progrÃ¨s notable par rapport au cadre antÃ©rieur.

Les mesures de sauvegardes additionnelles prÃ©vues par cetÂ *EO*Â sont jugÃ©es en effet constituer uneÂ *Â«Â amÃ©lioration significativeÂ Â»*,Â de mÃªme que lâ€™introduction des concepts de nÃ©cessitÃ© et de proportionnalitÃ© dans lâ€™encadrement juridique de lâ€™activitÃ© des agences de renseignementÂ ; le CEPD se satisfait aussi de ce que cetÂ *EO*Â prÃ©voit une liste de finalitÃ©s spÃ©cifiques pour lesquelles une collecte de donnÃ©es ne peut avoir lieu.

Le CEPD voit Ã©galement comme une amÃ©lioration significative par rapport au mÃ©canisme de

lâ€™Ombudsperson du Privacy ShieldÂ la crÃ©ation par cet ordre exÃ©cutif dâ€™un nouveau mÃ©canisme de recours pour les personnes concernÃ©es non amÃ©ricaines.Â Ce mÃ©canisme sâ€™articule en deux tempsÂ : le dÃ©pÃ´t dâ€™une plainte devant le Civil Liberties Protection Officier of the Office of the Director of National Intelligence (CLPO), puis une possibilitÃ© de faire appel devant un nouvel organisme, la Data Protection Review Court (DPRC). Le CEPD salue les pouvoirs plus Ã©tendus confÃ©rÃ©s Ã cetteÂ CourÂ pour remÃ©dier aux Ã©ventuelles violations constatÃ©es ainsi que son indÃ©pendance accrue en comparaison du systÃ¨me de lâ€™Ombudsperson. Il reconnaÃ®t Ã©galement lâ€™amÃ©lioration tenant aux garanties supplÃ©mentaires prÃ©vues dans le nouveau mÃ©canisme de recours, telles que le rÃ´le des avocats spÃ©ciaux, qui comprend la dÃ©fense des intÃ©rÃªts du plaignant, ainsi que lâ€™examen du mÃ©canisme de recours par le Privacy and Civil Liberties Oversight Board (PCLOB).

6. Les points dâ€™inquiÃ©tudeâ€“ Si les progrÃ¨s sont avÃ©rÃ©s et reconnus comme tels, le CEPD relÃ¨ve nÃ©anmoins de nombreux points mÃ©ritantÂ *Â«Â clarificationÂ Â»*etÂ *Â«Â attentionÂ Â»*, voire suscitantÂ *Â«Â lâ€™inquiÃ©tudeÂ Â»*.

Dâ€™un point de vue formel, le CEPD relÃ¨ve que la prÃ©sentation des annexes et leur numÃ©rotation rendent complexe la prÃ©sentation du Data Privacy FrameworkÂ ; cette remarque nâ€™est pas sans rappeler lâ€™exigence de clartÃ© et de lisibilitÃ© qui pÃ¨se sur les responsables de traitement lorsquâ€™ils fournissent une information aux personnes concernÃ©es. Lâ€™essentiel des remarques du CEPD a nÃ©anmoins trait au fond.

Sur la base de lâ€™expÃ©rience du Safe Harbor puis du Privacy Shield,Â le CEPD se montre tout dâ€™abord rÃ©servÃ© quant au mÃ©canisme dâ€™autocertification sur lequel repose le systÃ¨me et sâ€™inquiÃ¨te de son contrÃ´le effectif.

Quant aux principes applicables, le CEPD note que si le projet de dÃ©cision dâ€™adÃ©quation modifie et ajoute des explications dans ses considÃ©rants,Â les principes du Data Privacy Framework auxquels lesÂ Â«Â organisations DPFÂ Â»Â doivent adhÃ©rer restent cependant en substance les mÃªmes que ceux qui Ã©taient applicables sous le Privacy Shield.Â Or, ces principes ont dÃ©jÃ fait lâ€™objet dâ€™une analyse par le G29[6]Â Ã lâ€™Ã©poque oÃ¹ le projet du Privacy Shield Ã©tait discutÃ©, et le CEPD constate que des inquiÃ©tudes sur un ensemble de points clÃ©s dÃ©jÃ identifiÃ©s alors subsistent toujours.

Parmi ces points, le ComitÃ© relÃ¨ve que laÂ dÃ©finition de certains termes essentiels, comme celle dâ€™*Â«Â agentÂ Â»*Â et deÂ *Â«Â processorÂ Â»*, nâ€™est pas spÃ©cifiÃ©e et que la terminologie nâ€™est gÃ©nÃ©ralement pas utilisÃ©e de maniÃ¨re univoque dans le DPF. Le CEPD observe Ã©galement queÂ la mesure dans laquelle les principes du DPF sâ€™appliquent aux imporÂtateurs agissant seulement en qualitÃ© de sous-traitantÂ nâ€™est pas claire, dans la mesure oÃ¹ le DPF ne distingue pas les principes applicables Ã ces derniers de ceux applicables aux responsables du traitement, certains nâ€™Ã©tant manifestement applicables quâ€™Ã ceux-ci.

Un autre point dâ€™attention est pour le CEDP que lesÂ restrictions Ã lâ€™exportationÂ des donnÃ©es vers un pays tiers devraient Ãªtre clarifiÃ©es par la Commission.

Sâ€™agissant desÂ *Â«Â droits des personnes concernÃ©esÂ Â»*, le CEPD note que les principes relatifs au droit dâ€™accÃ¨s, identiques Ã ceux inscrits dans le Privacy Shield, font lâ€™objet des mÃªmes critiques quâ€™Ã lâ€™Ã©poque de lâ€™adoption de cette prÃ©cÃ©dente dÃ©cisionÂ :Â ce droit dâ€™accÃ¨s est conÃ§u dâ€™une maniÃ¨re Ã©triquÃ©e trop favorable Ã lâ€™importateurÂ ; il est par ailleurs neutralisÃ© dans lâ€™hypothÃ¨se oÃ¹ lâ€™information est publique ou bien figure dans des registres publics, ce que le CEPD regrette en faisant valoir que la personne concernÃ©e perd alors la possibilitÃ© de contrÃ´ler lâ€™exactitude des donnÃ©es et de vÃ©rifier si les donnÃ©es ont Ã©tÃ© lÃ©galement rendues publiques en premier lieu. Les modalitÃ©s du droit dâ€™opposition sont jugÃ©es insuffiÂ-samment prÃ©cisÃ©es et lâ€™hypothÃ¨se dâ€™un intÃ©rÃªt lÃ©gitime impÃ©rieux de la personne concernÃ©e au regard de sa situation particuliÃ¨re nâ€™est pas pris en compte. Le CEPD sâ€™inquiÃ¨te Ã©galement du fait que les rÃ¨gles sur les dÃ©cisions individuelles automatisÃ©es et le profilage semblent varier, lorsquâ€™elles existent, selon les secteurs considÃ©rÃ©sÂ ; il estime aussi que des rÃ¨gles spÃ©cifiques pour ces prises de dÃ©cision individuelles automatisÃ©es sont nÃ©cessaires afin de fournir des garanties suffisantes, y compris le droit de la personne concernÃ©e de connaÃ®tre la logique utilisÃ©e, de contester la dÃ©cision et dâ€™obtenir une intervention humaine quand la dÃ©cision lâ€™affecte dâ€™une faÃ§on significative.

Quant Ã la mise en Å“uvre des principes formulÃ©s dans le DPF, le CEPD recommande que la dÃ©cision dâ€™adÃ©quation soit rendue conditionnelle Ã lâ€™adoption par les agences de renseignement amÃ©ricaines de politiques et de procÃ©Âdures de mise en Å“uvre de lâ€™*EO*Â 14086, qui devront de surcroÃ®t Ãªtre surveillÃ©es par la Commission.

La portÃ©e des exceptions prÃ©vues Ã lâ€™obligation de respecter les principes du DPF (*comply with a court orderÂ ; public interestÂ ;Â law enforcementÂ ; national security requirement*) devrait Ã©galement Ãªtre clarifiÃ©e.

Parmi les points mÃ©ritant attention figurent Ã©galement les rÃ¨gles applicables Ã laÂ *Â«Â collecte temporaire en masseÂ Â»*[7]Â sous le rÃ©gime de lâ€™actuelÂ *EO*Â 12333, ainsi que la rÃ©tention et la dissÃ©mination de ces donnÃ©es dans le systÃ¨me juridique amÃ©ricain. Cette collecte, notamment, ne

rÃ©pond pas Ã lâ€™exigence dâ€™une autorisation prÃ©alable par une autoritÃ© indÃ©pendante, telle que requise dans la jurisÂprudence la plus rÃ©cente de la Cour europÃ©enne des droits de lâ€™homme (CEDH), ni Ã lâ€™exigence dâ€™un examen indÃ©pendant systÃ©matique a posteriori par un tribunal ou un organisme Ã©quivalent. En ce qui concerne lâ€™autorisation indÃ©pendante prÃ©alable de la surveillance au titre de la section 702 du FISA (Foreign Intelligence Surveillance Act), le CEPD regrette que la FISA Court (FISC) nâ€™examine pas la conformitÃ© dâ€™une demande de programme avec lâ€™*EO* Â 14086 lorsquâ€™elle certifie le programme autorisant le ciblage de personnes non amÃ©ricaines, alors que les autoÂritÃ©s de renseignement qui exÃ©cutent le programme sont liÃ©es par cetÂ *EO*. Selon le ComitÃ©, les garanties supplÃ©mentaires contenues dans cette ordonÂnance devraient nÃ©anmoins Ãªtre prises en compte, y compris par la FISC.

Lâ€™essentiel des autres remarques du CEPD a trait au mÃ©canisme de recours prÃ©vu par le Data Privacy Framework.

Le ComitÃ© considÃ¨re que le premier niveau du mÃ©caÂnisme de recours nâ€™est pas investi dâ€™un degrÃ© dâ€™indÃ©ÂpendanceÂ suffisantÂ pour satisfaire aux exigences de lâ€™article 47 de la Charte de lâ€™Union europÃ©enne sur le droit Ã un recours effectif et Ã lâ€™accÃ¨s Ã un tribunal impartial. Les personnes concernÃ©es sont Ã©galement censÃ©es soumettre leur plainte,*Â viaÂ* une autoritÃ© nationale europÃ©enne compÃ©tente, pour tout ce qui touche aux questions de sÃ©curitÃ© nationale ou de traitement de donnÃ©es par des autoritÃ©s publiques, ce que le CEPD regrette au regard de la diversitÃ© des situations en Europe Ã cet Ã©gard.

Quant au second niveau, le ComitÃ© relÃ¨ve que si la Data Protection Review Court est qualifiÃ©e deÂ Â«Â CourÂ Â», elle est Ã©tablie par unÂ *executive order*, ce qui prÃ©sente certains avantages, mais peut susciter une inquiÃ©tude quant Ã son indÃ©pendance rÃ©elle par rapport Ã lâ€™exÃ©cutifÂ ; le CEPD recommande Ã cet Ã©gard Ã la Commission de surveiller la mise en Å“uvre concrÃ¨te des rÃ¨gles qui sont destinÃ©es Ã assurer son indÃ©pendance. Le CEPD sâ€™inquiÃ¨te Ã©galement de la maniÃ¨re dont la DPRC statue. Le plaignant nâ€™aura en effet pas le droit de savoir sâ€™il a suscitÃ© lâ€™intÃ©rÃªt des services de renseignement, mais simplement celui dâ€™Ãªtre informÃ©, soit de ce quâ€™aucune violation couverte par le DPF nâ€™a Ã©tÃ© identifiÃ©e, soit quâ€™une dÃ©cision exigeant un remÃ¨de appropriÃ© a Ã©tÃ© prise,Â la dÃ©cision nâ€™Ã©tant pas susceptible de recours. Le CEPD sâ€™inquiÃ¨te enfin de lâ€™incertitude sur ce qui pourra constituer ce que lâ€™*EO*Â 14086 qualifie deÂ *Â«Â remÃ¨de appropriÃ©Â Â»*Â pour la personne concernÃ©e lorsquâ€™une violation est constatÃ©e.

On voit ainsi que, dans lâ€™ensemble, si le CEPD nâ€™hÃ©site pas Ã souligner les amÃ©liorations importantes apportÃ©es au systÃ¨me du Privacy Shield, il regrette que certains sujets de prÃ©occupation, identifiÃ©s avant lâ€™adoption de ce dernier, ne soient toujours pas pris en compte, et souligne dâ€™autres motifs de prÃ©occupation quant au nouveau cadre proposÃ©.

7. Lâ€™opinion du Parlement europÃ©enâ€“ La Commission des libertÃ©s civiles, de la justice et des

affaires intÃ©rieures (LIBE) du Parlement europÃ©en a quant Ã elle fait preuve de moins de subtilitÃ© dans lâ€™expression de son opinion sur le projet de dÃ©cision dâ€™adÃ©quationÂ : dans un document de travail datÃ© du 14Â fÃ©vrier 2023[8],Â elle a estimÃ© que ce projetÂ *Â«Â Ã©choue Ã proposer une vÃ©ritable Ã©quivalence dans le niveau de protectionÂ Â»*requis par le droit europÃ©en de la protection des donnÃ©es et de la Charte de lâ€™Union europÃ©enne telle quâ€™interprÃ©tÃ©e par la CJUE.

Cette opinion vient dâ€™Ãªtre reprise par le Parlement europÃ©en dans une rÃ©solution[9]Â du 11Â mai 2023 adoptÃ©e Ã la faveur de 306 voix pour, 27 contre et 231 abstentions.

Le Parlement estime que si les Ã‰tats-Unis ont fait preuve dâ€™un engagement certain pour amÃ©liorer les rÃ¨gles et remÃ¨des applicables au traitement de donnÃ©es par les autoritÃ©s publiques amÃ©ricaines, les principes du Privacy Shield nâ€™ont pas Ã©tÃ© suffisamment amendÃ©s pour assurer la protection Ã©quivalente requise. Par ailleurs, Ã©tant donnÃ© que, dâ€™une part, les services amÃ©ricains de renseignement ont jusquâ€™en octobre 2023 pour mettre Ã jour leurs politiques et pratiques afin de se conformer Ã lâ€™*EO*Â 14086, et que, dâ€™autre part, lâ€™avocat gÃ©nÃ©ral amÃ©ricain doit encore dÃ©signer lâ€™Union europÃ©enne et ses Ã‰tats membres comme des pays remplissant les conditions requises pour avoir accÃ¨s Ã la DPRC, la Commission nâ€™Ã©tait pas en mesure dâ€™Ã©valuerÂ *Â«Â en pratiqueÂ Â»*Â lâ€™efficacitÃ© des mesures correctives et des mesures proposÃ©es en matiÃ¨re dâ€™accÃ¨s aux donnÃ©es. Il en conclut que la Commission ne saurait adopter une dÃ©cision dâ€™adÃ©quation que lorsque les Ã‰tats-Unis auront dâ€™abord respectÃ© ces dÃ©lais, et franchi ces Ã©tapes, afin de garantir que les engagements ont Ã©tÃ© tenus dans la pratique.

Si cette rÃ©solution a Ã©tÃ© adoptÃ©e par un vote Ã lâ€™occasion duquel de nombreux parlementaires se sont abstenus, on peut toutefois raisonnablement penser que cette circonstance nâ€™enlÃ¨ve rien Ã son poids politique et mÃ©diatique, dâ€™autant plus que cette rÃ©solutionÂ Â«Â nÃ©gativeÂ Â»Â vient sâ€™ajouter aux rÃ©serves prÃ©cÃ©demment exposÃ©es du CEPD, lâ€™expert europÃ©en en matiÃ¨re de protection des donnÃ©es.

8. Situation de la CommissionÂ â€“ La Commission euroÂpÃ©enne se trouve dans une position dÃ©licate, mÃªme si chacune des institutions prÃ©citÃ©es a su laisser desÂ Â«Â portes ouvertesÂ Â»Â Ã lâ€™adoption dâ€™une dÃ©cision dâ€™adÃ©quation qui puisse Ãªtre satisfaisante Ã leurs yeux.

Ne tenir aucun compte des recommandations et inquiÃ©Âtudes formulÃ©es serait sans doute trop dangereux, car une potentielle troisiÃ¨me invalidation par la CJUE dâ€™une dÃ©cisiondâ€™adÃ©quation rendue en faveur du cadre transatlantique Ã©laborÃ© par ses soins serait assez infaÂmante. Ne rien faire serait dâ€™autant plus dangereux que lâ€™on peut nourrir de rÃ©elles interrogationssur la maniÃ¨re concrÃ¨te dont les agences amÃ©ricaines mettront en Å“uvre lâ€™*EO*Â 14086, de mÃªmeque sur la capacitÃ© du nouveau mÃ©canisme de recours proposÃ© Ã satisfaire en lâ€™Ã©tat auxexigences de lâ€™article 47 de la Charte de lâ€™UE tel quâ€™interprÃ©tÃ© par la CJUE.

Il est donc probable que la Commission attende au minimum dâ€™obtenir des prÃ©cisions de la part de la communautÃ© du renseignement amÃ©ricain sur la maniÃ¨re dont cette derniÃ¨re entend mettre en Å“uvre les nouvelles garanties prÃ©vues par lâ€™ordre exÃ©cutif 14086Â ; il lui seraÂ sans doute plus difficile dâ€™obtenir une amÃ©lioration du mÃ©canisme de recours nÃ©gociÃ© avec les autoritÃ©s amÃ©ricaines, mÃªme si lâ€™on ne peut Ã©videmment lâ€™exclure.

9. Pourquoi tant de difficultÃ©sÂ ?â€“ Toute cette discussion sâ€™inscrit sur une toile de fond que lâ€™on perd de vue Ã force de se focaliser sur les aspects techniques des systÃ¨mes successivement proposÃ©s. Il nâ€™est pas inutile de rappeler le contexte tant on peut penser quâ€™il est Ã lâ€™origine des difficultÃ©s constatÃ©es depuis une dizaine dâ€™annÃ©es.

Si le CEPD, Ã la suite de la CJUE, insiste sur le fait quâ€™on ne saurait exiger dâ€™un pays tiers, pour quâ€™il puisse faire lâ€™objet dâ€™une dÃ©cision dâ€™adÃ©quation, quâ€™il adopte un systÃ¨me de protection des donnÃ©esÂ *Â«Â identiqueÂ Â»*Â Ã celui de lâ€™Union europÃ©enne,Â il reste que lâ€™on peut raisonnablement imputer la difficultÃ© de la Commission et des autoritÃ©s amÃ©ricaines Ã crÃ©er un cadre qui puisse Ãªtre considÃ©rÃ© comme satisfaisant par la CJUE aux diffÃ©rences de fond trop importantes entre les Ã‰tats-Unis et lâ€™Europe quant Ã lâ€™impÃ©ratif et Ã la maniÃ¨re de protÃ©ger les donnÃ©es Ã caractÃ¨re personnel.

LÃ oÃ¹ lâ€™Europe sâ€™est dotÃ©e dâ€™une lÃ©gislation gÃ©nÃ©rale et uniforme protÃ©geant par principe toute donnÃ©e qualifiable deÂ *Â«Â donnÃ©e Ã caractÃ¨re personnelÂ Â»*, les Ã‰tats-Unis ne connaissent majoritairement que des protections sectorielles. Certains Ã‰tats ont certes adoptÃ© des textes plus gÃ©nÃ©raux, mais on ne saurait dire pour la plupart quâ€™ils confÃ¨rent une protection comparable Ã celle que garantit le RGPDÂ ; au demeurant, des exceptions rÃ©duisent leur champ dâ€™application et, mÃªme lorsquâ€™ils se trouvent applicables, les consÃ©quences dâ€™une violation ne sont pas nÃ©cessairement dissuasives.

Si lâ€™approche sectorielle peut Ã la rigueur sâ€™expliquer par une diffÃ©rence de culture juridique â€“ laÂ *Common Law*Â fonctionne en rÃ©glant des cas particuliers plutÃ´t quâ€™en posant des rÃ¨gles gÃ©nÃ©rales â€“, les autres aspects sâ€™expliquent fondamentalement parÂ le fait que lesÂ Ã‰tats-Unis voient dans une protection de type euroÂpÃ©enÂ non seulement une protection trop absolue des donnÃ©es Ã caractÃ¨re personnel, mais aussi et surtout un frein Ã lâ€™activitÃ© Ã©conomique et Ã la

prospÃ©ritÃ©Â :Â il sâ€™agit pour les entreprises dâ€™une dÃ©pense vue comme compromettant inutilement leur compÃ©titivitÃ©. Ã€ cela, il faut ajouter que les Ã‰tats-Unis sont historiquement hostiles Ã tout engagement international restreignant leur libertÃ© dâ€™actionÂ ; or, il est ici question de refrÃ©ner lâ€™action de leurs puissants services de renseignement.

Ceci a pour consÃ©quence, en somme, que les Ã‰tats-Unis ne cherchent pas tant Ã se rapprocher des principes europÃ©ens de la protection des donnÃ©es quâ€™Ã crÃ©er dans leur systÃ¨me juridique un rÃ©gime spÃ©cial propre Ã contenter les exigences europÃ©ennes, mais dans les limites les plus strictes par rapport Ã leurs propres conceptions. On sâ€™expliÂque alors quâ€™il ne soit pas sÃ»r que le troisiÃ¨me projet proposÃ© prÃ©sente enfin toutes les garanties requises par la CJUEÂ : lâ€™expÃ©rience montre que chaque Ã©volution dans le sens requis par lâ€™Europe semble Ãªtre une concession arrachÃ©e et, en consÃ©quence, insuffisamment complÃ¨te pour remplir pleinement lâ€™exigence quâ€™elle a pour objet de satisfaire.

Cette diffÃ©rence de culture en matiÃ¨re de protection des donnÃ©es, au-delÃ des points techniques soulevÃ©s par le CEPD et les membres du Parlement europÃ©en, explique fondamentalement la difficultÃ© de lâ€™exÃ©cutif amÃ©ricain et de la Commission Ã mettre en place un systÃ¨me pouvant satisfaire la CJUEâ€¦ et Maximilien Schrems, dont on ne saurait douter quâ€™il prÃªtera son nom Ã un troisiÃ¨me arrÃªt de la Cour de justice sur la question.

SourcesÂ :

1. CJUE, 6 octobre 2015, C-392/14, Maximilian Schrems *v* Data Protection Commissioner.
2. CJUE, 16 juillet 2020, C-311/18, Data Protection Commissionner c. Facebook Ireland Ltd, Maximilian Schrems.
3. Voir le site de la Commission europÃ©enne, commission.europa.eu
4. Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework.
5. Executive Order 14086â€”Enhancing Safeguards for United States Signals Intelligence Activities, Oct. 7th 2022.
6. Le groupe de travail de lâ€™article 29 ou G29 sous lâ€™Ã©gide de la directive 95/46 du 24 octobre 1995 sur la protection des donnÃ©es personnelles est le prÃ©dÃ©cesseur du ComitÃ© europÃ©en Ã la protection des donnÃ©es (CEPD) sous lâ€™Ã©gide du RGPD.
7. *Â« temporary bulk collection Â»*
8. Draft motion for a resolution to wind up the debate on the statement by the Commission pursuant to Rule 132(2) of the Rules of Procedure on the adequacy of the protection afforded by the EU-US Data Privacy Framework (2023/2501(RSP)), nÂ° 11.
9. European Parliament resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-US Data Privacy Framework.

Categorie

1. Droit

date crÃ©Ã©e
29 aoÃ»t 2023
Auteur
audit