CNNum
Conseil National du Numérique

Communiqué

Pourquoi l'accord « *Privacy Shield* » doit être renégocié

L'accord « Privacy Shield » organise une partie du transfert des données entre l'Union européenne et les États-Unis. Il fait actuellement l'objet d'une évaluation annuelle. En prévision de cette échéance, les membres du Conseil ont reçu une délégation américaine durant l'été pour échanger sur les différents enjeux du dispositif et formuler leurs interrogations. Le Conseil s'associe aux vives inquiétudes déjà exprimées par le G29, la délégation de la commission des libertés civiles (LIBE) du Parlement européen et un grand nombre d'associations de défense des droits : le « Privacy Shield » présente un trop grand nombre de zones d'ombres et ne donne pas suffisamment de garanties à la protection des données personnelles des Européens. Conformément à l'engagement du candidat Emmanuel Macron, cet accord doit être renégocié pour organiser une circulation des données sécurisée, respectueuse de nos droits et libertés et favorable aux entreprises. L'économie européenne a besoin d'avoir un cadre équitable et stable, et non pas d'un accord faible, susceptible d'annulation sur les mêmes fondements que son prédecesseur. Une telle mesure serait préjudiciable, tant pour les citoyens que pour les entreprises françaises et européennes, qui ont besoin de sécurité juridique.

Les questions liées à la surveillance restent entières

Lors des négociations sur l'accord « *Privacy Shield* », la Commission européenne avait obtenu, de la part des autorités américaines, la promesse que la collecte de données ciblée resterait prioritaire sur la collecte de masse[1]. Pour cause : les pratiques de renseignement américain, mises au jour par les révélations d'Edward Snowden, étaient au cœur de la décision de la Cour de justice européenne invalidant le précédent accord sur le transfert de données entre les États-Unis et l'Union européenne (accord dit « *Safe Harbor* »). Cette avancée est néanmoins toute relative car il ne s'agit en réalité que d'une simple directive présidentielle. Cette promesse n'est pas inscrite « en dur » et le droit américain reste largement inchangé. Il en va

[1] Si cette dernière doit avoir lieu, elle doit être « aussi ajustée que possible » (« *as tailored as feasible* »).

ainsi de la portée de la collecte, qui peut toujours être justifiée à des fins « sécurité nationale », un motif comprenant des objectifs aussi larges que non-définis[2].

Les évolutions législatives et jurisprudentielles récentes (voir annexes), combinés à la position affichée par la nouvelle administration, jettent un éclairage nouveau sur le dispositif. Si ces développements ne remettent pas fondamentalement en cause l'équilibre juridique (au demeurant très perfectible) de la protection des données aux États-Unis, ils constituent à tout le moins un signal politique particulièrement préoccupant. La vigilance doit être de mise. Le Conseil restera attentif aux futures évolutions américaines, en particulier la reconduction éventuelle du titre VII du FISA Amendments Act (FAA) américain, censé expirer à la fin de l'année. Ces dispositions comprennent la controversée « section 702 », qui permet la surveillance très large de tout ressortissant d'un pays étranger. Cette section a également servi de fondement aux programmes PRISM et UPSTREAM.

Le Conseil s'associe par ailleurs aux vives inquiétudes exprimées par de nombreuses parties prenantes avant lui sur la vacance de nombreux postes clés en charge de l'administration et de la supervision du dispositif côté américain et sur l'effectivité des mécanismes de recours.

Asymétrie critique

À la question — essentielle — du respect de la vie privée des citoyens européens s'ajoutent des considérations plus économiques. Les données constituent un actif essentiel de l'économie numérique. Elles sont un levier majeur de création de valeur, d'innovation et de croissance, non seulement pour le secteur des technologies de l'information mais aussi pour un nombre grandissant et quasi généralisé de filières économiques. Dans un contexte d'asymétrie très forte entre les industries numériques européennes encore naissantes et les géants extra-européens, le précédent accord dit « *Safe Harbor* » a contribué à renforcer ce déséquilibre. Les contrôles, particulièrement faibles, liés aux mécanismes d'auto-certification ont pu entraîner une perte de compétitivité pour les entreprises européennes, soumises à des exigences plus strictes. Dans ce contexte, l'entrée en vigueur prochaine du règlement général pour la protection des données (RGPD), qui renforce les obligations des entreprises opérant sur le territoire européen, conduit au même risque de déséquilibre.

Il est essentiel de ne pas faire preuve de naïveté et de ne pas répéter les erreurs du passé. La position de prédominance des acteurs extra-européens sur le territoire de l'Union peut à ce titre justifier une approche prioritairement défensive.

L'accord « *Privacy Shield* » doit ainsi être conçu comme un dispositif transitoire. Il est nécessaire de s'atteler à la négociation d'un accord plus robuste juridiquement, pour garantir la protection des données personnelles de tous les européens, dans un cadre suffisamment stable pour nos entreprises. Il s'agit également de prendre la pleine conscience de l'asymétrie existante en matière de flux de données entre les États-Unis et l'Union

[2] On retrouve notamment parmi ces motifs le contre-terrorisme, le contre-espionnage, la cyber-sécurité, la protection des forces armées ou encore la lutte contre la criminalité transnationale.

européenne. L'entrée en vigueur, l'an prochain, du RGPD et l'harmonisation des législations nationales, doit permettre cette négociation sur des bases plus solides.

Le Conseil.

Le Conseil national du numérique est une commission consultative indépendante. Ses membres ont été nommés par un décret du Président de la République du 8 février 2016. Le Conseil national du numérique a pour mission de formuler de manière indépendante et de rendre publics des avis et des recommandations sur toute question relative à l'impact du numérique sur la société et sur l'économie.

Contact presse.

Yann Bonnet
Secrétaire général
presse@cnnumerique.fr
01 53 44 21 27

www.cnnumerique.fr
@CNNum

Annexes

1. Les récents développements américains en matière de protection des données jettent un jour nouveau sur l'accord Privacy Shield.

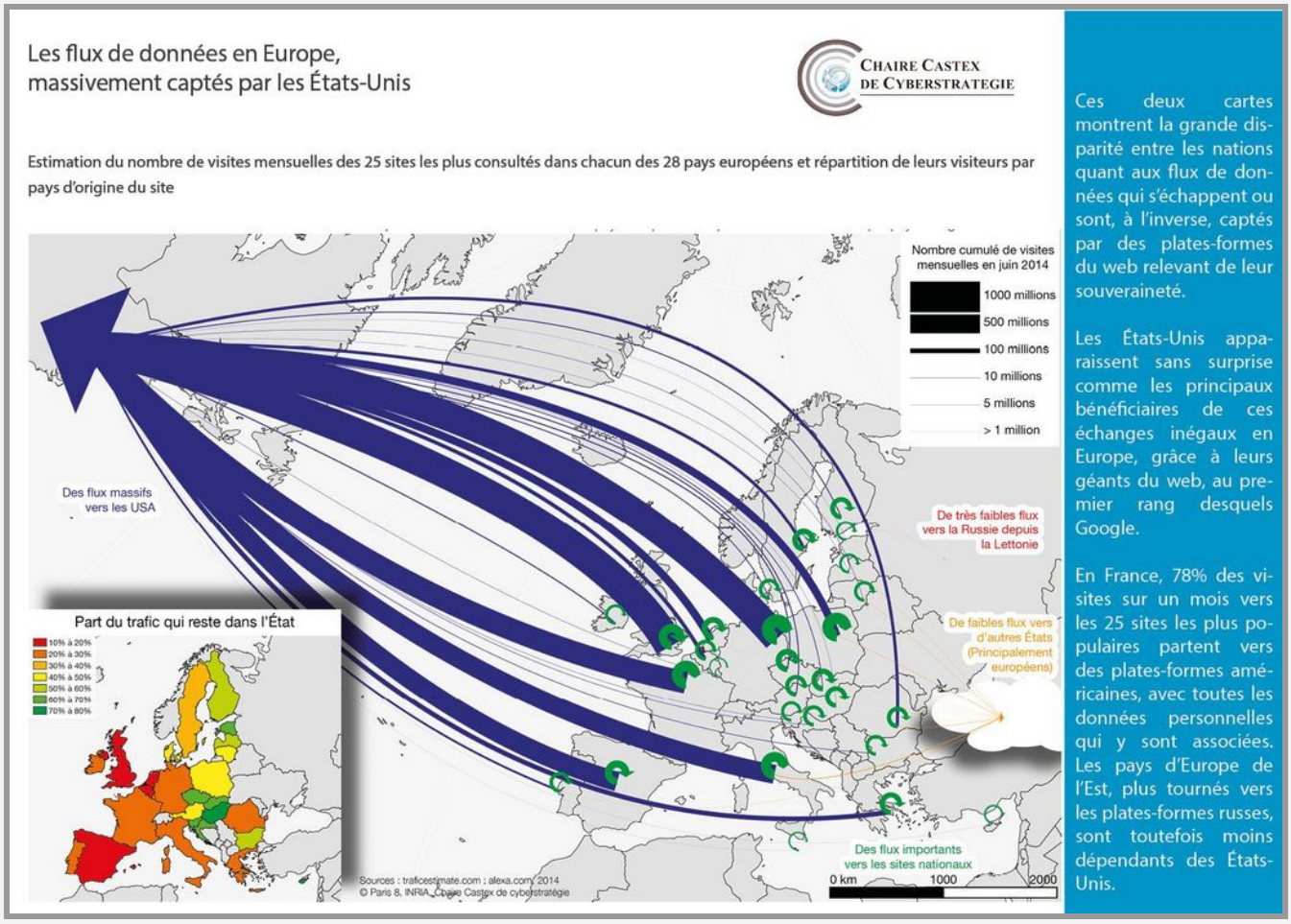
- Les révélations concernant les activités d'espionnage conduites par un fournisseur américain de services de communications électroniques, à la demande de la NSA et du FBI en 2015, un an après que la directive présidentielle était censée limiter la quantité de données pouvant être collectées et traitées ;

- Un décret présidentiel de la nouvelle administration prévoyant que « *les agences* [comme la NSA et le FBI] *devront, dans la mesure permise par la loi en vigueur, s'assurer que leurs politiques de protection des données personnelles excluent les non-citoyens américains et les non-résidents permanents autorisés, des protections offertes par le Privacy Act au regard des informations personnelles identifiables.* » ;

- Les nouvelles règles permettant à la NSA, depuis janvier 2017, de partager avec 16 autres agences, dont le FBI, de grandes quantités de données personnelles collectées sans mandat ni décision de justice ou autorisation du Congrès ;

- Le rejet par le Sénat et la Chambre des représentants, en mars 2017, de règles protégeant les consommateurs de services à haut débit, éliminant ainsi « *des règles qui auraient obligé les fournisseurs d'accès à internet de demander l'accord formel de leurs clients avant de vendre ou de partager des données de navigation internet ainsi que d'autres informations privées avec les annonceurs et d'autres sociétés privées* ».

2. Les flux de données en Europe massivement captés par les États-Unis.



Source : Chaire Castex de Cyberstratégie