Construire une souveraineté numérique européenne

La Cour de Justice de l'Union Européenne, en juillet dernier, a invalidé le Privacy Shield, adopté en 2016 par la Commission européenne pour remplacer le Safe Harbor. Ce dispositif était censé garantir un standard de traitement conforme aux exigences du Régime Général de Protection des Données (RGPD) aux informations stockées par des hébergeurs américains, mais la CJUE a noté que cela n'était en réalité pas le cas.

Avec Florian Gerard-Mercier
Avec Geoffroy de Neuville

Alors que Donald Trump a signé des décrets présidentiels interdisant l'application TikTok aux Etats-Unis si elle n'est pas rachetée par une entreprise américaine d'ici au 20 septembre (Microsoft est déjà sur les rangs), et que les dirigeants des GAFA ont passé le 30 Juillet une audition difficile face au Congrès américain pour leurs pratiques anticoncurrentielles, de ce côté-ci de l'Atlantique, la Cour de Justice de l'Union Européenne a également tapé fort du poing sur la table le 16 juillet dernier dans l'affaire dite « Shrems ». Elle a en effet invalidé le *Privacy Shield,* adopté en 2016 par la Commission européenne pour remplacer le*Safe Harbor* – déjà très critiqué. Ce dispositif était censé garantir un standard de traitement conforme aux exigences du Régime Général de Protection des Données (RGPD) aux informations stockées par des hébergeurs américains, mais la CJUE a noté que cela n'était en réalité pas le cas.

Le *Privacy Shield*, un projet en réalité mort-né ?

Les juges de la CJUE avaient dans leur ligne de mire deux cibles. En premier lieu, les garanties de protection quant au traitement général (accès et usage) des données à caractère personnel par la règlementation américaine qui ne répondaient plus aux standards minimums européens. Les programmes américains de surveillance des données utilisateur explicitement dénoncés dans l'arrêt excèdent le « strict nécessaire » selon les dires de la Cour, rendant caduc l'argument d'autorité de la « sécurité nationale » et de l'intérêt public qui étaient alors brandis pour justifier ces ingérences douteuses. En second lieu, l'insuffisante protection juridictionnelle des individus en cas de violation de leurs droits à la protection de leurs données. L'indépendance douteuse du médiateur américain chargé des litiges n'était plus assurée et privait alors le requérant de garanties procédurales équivalentes à celles requises par l'UE.

Les transferts de données à destination des Etats-Unis sur le fondement du*Privacy Shield* sont donc désormais illicites. L'invalidation du *Privacy Shield* est ainsi un séisme juridique, mais aussi politique en envoyant un signal fort aux géants de la tech américaines. Néanmoins, si l'on souhaite éviter une redite de l'échec du passage du *Privacy shield* pour remplacer le *Safe harbour*, puis du retoquage récent du *Privacy shield*, il convient d'adopter une approche plus globale et d'organiser une riposte européenne à plusieurs niveaux.

Le premier problème est d'ordre structurel puisqu'il réside dans notre hyper dépendance aux services numériques proposés par des entreprises de nationalité américaine : Google, Amazon, Facebook, Apple et Microsoft. Or, ces services, hébergés aux USA par des entreprises américaines, se trouvent logiquement soumis à l'ordre juridique américain. Intrinsèquement, la protection des données européennes traitées par des services américains aux USA ne serait donc possible que si les USA renonçaient volontairement à leur

souveraineté pour aligner leur droit sur celui européen. C'est ce que semblait naïvement espérer imposer le *Privacy Shield*, et c'est pour cela qu'il s'est logiquement soldé par un échec cuisant.

Cet échec n'est pas étonnant : rétrospectivement, on peut s'interroger sur l'authenticité des « bons sentiments » du législateur américain quant à sa volonté d'apporter des protections équivalentes au RGPD : 2 mois avant son entrée en vigueur le 25 mai 2018, le parlement américain se postait en contre-offensive en promulguant le *Cloud Act* lequel exige que

Le second problème pour la souveraineté numérique européenne est, si l'on s'en donne les moyens, d'ordre conjoncturel : c'est le lieu physique d'hébergement et de traitement des données. En effet, si les données européennes traitées par des services américains l'étaient sur des serveurs européens, alors l'Europe pourrait garantir sa souveraineté et la sécurité de ces données. La faiblesse numérique actuelle de l'Europe vient donc aussi du fait que près de quatre serveurs sur dix sont physiquement localisés sur le territoire américain exposant ainsi nos données au principe de territorialité : quasiment toutes les données internet européennes transitent en effet par les USA. De même, l'Europe reste aussi très exposée à la domination américaine du fait de la répartition du marché des *cloud services* : Google, Apple et Facebook absorbent à eux seuls 85% du marché du*cloud.*

Se donner les moyens d'imposer une interdiction de l'exportation des données personnelles européennes hors d'Europe

Une réponse globale européenne devrait donc d'abord se doter d'une politique industrielle permettant la création d'acteurs européens de l'hébergement de données et des *cloud services* d'une taille suffisante pour que l'on puisse ensuite imposer aux services numériques étrangers l'interdiction de l'exportation ou du transit de données personnelles européennes hors de l'Union Européenne.

En effet, à l'ère du « tout digital », il est capital de bien comprendre le lien entre le quasi-monopole des sociétés de la*tech* américaines – le fait – et notre exposition aux lois américaines – le droit. Pour cela, il faut brièvement mettre en exergue la théorie des compétences internationales de l'Etat. Plus simplement dit : dans quel cas un Etat peut-il prétendre régir une situation ? La territorialité des lois et des juridictions veut qu'un Etat ne puisse pas régir sans limite des situations qui lui seraient trop éloignées en vertu de la souveraineté légale et judiciaire de ses pairs. Ainsi, les situations en dehors du territoire national ne peuvent être soumises à la loi d'un pays qu'à condition qu'il existe un lien de rattachement pertinent avec ledit territoire. La nationalité (compétence personnelle) ou encore la présence sur le territoire (compétence territoriale) sont les deux points de contact les plus connus. Ainsi, l'exposition de nos données aux lois américaines est fonction du nombre de rattachements avec leur territoire, et c'est pour cela qu'il est capital que l'Europe adopte, en matière numérique, une politique globale de découplage maximal vis-à-vis des Etats-Unis.

Ce découplage signifierait la mort d'une certaine idée de l'internet, ouvert, universel, libre des contraintes étatiques. Néanmoins, il y a bien longtemps que cette utopie est morte et enterrée. En réalité, la Chine, quand elle a fermé son internet aux services américains, a montré la voie à nombre de pays en développement, qui ont eux-aussi refermé leur internet. L'interdiction ou le rachat de TikTok aux USA est le signe que cette boucle est bouclée, avec les pères de l'internet ouvert, les USA, refermant également leur réseau sur un modèle continental. L'Europe, si elle parvient à rapatrier l'hébergement et le traitement de ses données, et qu'elle fait la preuve que la RGPD fonctionne et permet de garantir la protection des données personnelles, pourrait alors non seulement recouvrer sa souveraineté numérique, mais également, si elle étend ses garanties de protection aussi aux données étrangères, devenir un sanctuaire pour les données de pays tiers désireux de s'émanciper du contrôle américain ou chinois. Dans l'affrontement qui se joue entre Chine et Etats-Unis, l'Europe pourrait alors servir de zone neutre et protégée pour les données du monde entier, une sorte de « Suisse de la donnée » qui permettrait de garder vivante la flamme d'un internet comme outil d'émancipation et non de contrôle.

Florian Gerard-Mercier, Directeur des études du Millénaire, think-tank spécialisé en politiques publiques et travaillant à refondation de la droite.

Geoffroy de Neuville, Expert auprès du Millénaire, doctorant en droit international.