GÉOPOLITIQUE DES DONNÉES : VERS UN NOUVEAU *PRIVACY SHIELD* ?

Compte-rendu du séminaire organisé par l'IRIS, le 8 mars 2023, avec le soutien de Google

En invalidant l'accord de transferts de données entre l'Union européenne et les États-Unis (*Privacy Shield*) par son arrêt « Schrems 2 » du 16 juillet 2020, la Cour de Justice de l'Union européenne (CJUE) a soulevé deux enjeux fondamentaux : la nécessaire amélioration du cadre de protection des données européennes lorsqu'elles transitent vers les États-Unis et la pérennisation du cadre juridique garantissant la légalité de ces transferts, afin que les économies européenne et américaine ne pâtissent plus de cette situation.

Depuis lors, la Commission européenne et le gouvernement fédéral américain ont progressé vers une nouvelle solution, matérialisée, du côté de Washington, par l'*Executive Order 14086* du 7 octobre 2022. Le 13 décembre dernier, la Commission européenne a publié un projet de décision d'adéquation devant déboucher sur un nouveau cadre de protection des données entre l'Union et les États-Unis.

LES ENTREPRISES IMPACTÉES PAR L'INVALIDATION DU *PRIVACY SHIELD*

Confrontées au risque de sanction par les autorités nationales de protection des données, les entreprises américaines, mais aussi européennes, se trouvent dans une position particulièrement inconfortable. Face à l'invalidation du *Privacy Shield*, les solutions de repli viennent à manquer. Souvent avancée, l'option du chiffrement des données est non seulement un pis-aller, mais également une solution insuffisante quand nombre de sous-traitants ont besoin d'avoir accès à des données « en clair ». À défaut, il est demandé aux entreprises de mener leurs propres analyses quant à l'adéquation des législations de dizaines de pays au regard du cadre juridique européen, en particulier du règlement général sur la protection des données (RGPD). Situation paradoxale de « privatisation de la conformation », selon un intervenant, dans laquelle des entreprises se retrouvent à la fois juges et parties.

LA RECHERCHE D'UN ÉQUILIBRE ENTRE PROTECTION DES DONNÉES ET SÉCURITÉ NATIONALE

À l'heure où s'opposent, d'un côté, les exigences de protection des données personnelles européennes, et de l'autre, l'impératif de sécurité nationale américain, c'est la voie d'un équilibre que recherchent les partenaires transatlantiques. Lors de ce séminaire, les différents intervenants se sont montrés plutôt optimistes, eu égard aux dernières avancées des négociations. Les principes de nécessité et de proportionnalité dans la collecte de données, et

l'établissement d'une liste d'objectifs légitimes pour de telles activités, par les services de renseignement, ont été pris en compte par les autorités américaines. En outre, il est désormais prévu qu'un nouveau mécanisme de recours pour les personnes concernées dans l'Union européenne soit mis sur pied, assorti de garanties supplémentaires : l'examen des recours par la Commission de surveillance de la vie privée et des libertés civiles (PCLOB) et, pour compenser le secret du contradictoire, l'intervention d' « avocats spéciaux » (*special advocates*) afin de représenter les individus, qui auront accès gratuitement à toutes les informations nécessaires pour défendre leurs mandants. Ces garanties sont parfois plus protectrices, a fait valoir un intervenant, que ce qui existe dans certains États membres de l'Union européenne pour le contrôle des interceptions légales.

VERS UNE APPROCHE « PAR LES RISQUES » ?

Face aux réserves (modérées) du Comité européen de protection des données et (plus strictes) de la commission des libertés civiles du Parlement européen, les intervenants ont souligné l'intérêt d'adopter une approche par les risques en la matière, dans le droit fil de la législation européenne (article 24 du RGPD). Le risque zéro étant par nature inatteignable, il importe de se référer au degré de gravité et de probabilité d'une atteinte à la protection des données personnelles des Européens dans le cadre des transferts de données transatlantiques – et non d'adopter une approche « principielle ». À cet égard, l'un des intervenants rappelle que l'arrêt « Schrems 2 » de la CJUE invoque la prise en compte des « expériences passées » pour mener l'évaluation de ces risques. Autrement dit, à quel rythme et dans quelles proportions un responsable de traitement de données personnelles a-t-il été confronté à des pratiques problématiques ? Sous cet angle, et contre une interprétation extensive de l'arrêt Schrems 2, un transfert de données ne présentant *a priori* pas d'intérêt pour les services de renseignement ne devrait pas pâtir de mesures répressives ou comminatoires.

C'est en maintenant un subtil équilibre entre un haut degré de protection des données, l'impératif de sécurité nationale et les nécessités économiques, dans un contexte d'étroites dépendances entre l'UE et les États-Unis, que la décision d'adéquation de la Commission européenne devrait être adoptée avant l'été.

ET ENSUITE ?

S'il est probable que la décision d'adéquation advienne prochainement, d'autres questions demeurent en suspens ; deux d'entre elles ont rapidement été évoquées par les intervenants.

D'une part, l'analyse de l'adéquation des législations d'autres pays pourrait contraindre un peu plus les transferts de données à l'étranger, bien que l'influence internationale du RGPD tende progressivement à niveler les particularismes juridiques. *Quid* d'un pays comme la Chine, qui désormais se prévaut de mieux respecter les droits garantis par le RGPD que les États-Unis ? D'autre part émerge, depuis quelques années, le problème de l'accès à distance de données stockées en Europe, notamment dans le cadre du *CLOUD Act* américain. Si ce dernier vise à éliminer les conflits de juridiction et à assurer une meilleure coopération judiciaire bilatérale, la possibilité d'accéder à des données stockées dans des serveurs situés hors des frontières américaines pose question, comme en témoigne l'affaire « Health Data Hub ». Des négociations ont cours actuellement entre la Commission européenne et le Gouvernement fédéral pour traiter ce problème et parvenir, à terme, à un accord bilatéral (*executive agreement*). À ce sujet, un intervenant est venu préciser la portée du CLOUD Act, en insistant sur les limites de son champ d'intervention : les demandes de production et de conservation de preuves émises par des autorités judiciaires, soit des données précises et circonscrites à des cas limités. À cet égard, le même intervenant souligne qu'une procédure de découverte, en droit de la concurrence, demande ainsi la production de données en bien plus grand nombre qu'une demande émanant d'autorités judiciaires. En outre, il relève qu'avec le règlement *e-Evidence* adopté en janvier 2023, l'Europe s'est dotée des mêmes pouvoirs que le *CLOUD Act*.

L'expertise stratégique en toute indépendance

2 bis, rue Mercœur - 75011 PARIS / France

+ 33 (0) 1 53 27 60 60

contact@iris-france.org

iris-france.org

L'IRIS, association reconnue d'utilité publique, est l'un des principaux think tanks français spécialisés sur les questions géopolitiques et stratégiques. Il est le seul à présenter la singularité de regrouper un centre de recherche et un lieu d'enseignement délivrant des diplômes, via son école IRIS Sup', ce modèle contribuant à son attractivité nationale et internationale.

L'IRIS est organisé autour de quatre pôles d'activité : la recherche, la publication, la formation et l'organisation d'évènements.