Les prémices d'un nouvel encadrement des transferts de données personnelles entre les États-Unis et l'Union européenne

La problématique du transfert des données personnelles a toujours été un enjeu économique considérable pour les entreprises. Le développement de l'ère de l'économie numérique a contribué à soulever des questionnements auprès des particuliers dans la collecte de leurs données. Les doutes ont été encore plus forts concernant les Etats dans le cadre du transfert des données de leur ressortissants vers des pays tiers.

Le partage des données hors de l'Union européenne s'est davantage développé avec l'explosion du e-commerce, mais aussi des réseaux sociaux, plateformes de collecte considérable de données.

En ce sens, on ne peut passer à côté de l'amende historique de 405 millions de dollars qu'*Instagram* a écopé le 5 septembre 2022 pour défaut de sécurisation des données de ses utilisateurs mineurs.

On remarque donc aisément le durcissement de la politique des Etats en matière de protection des données personnelles.

Ainsi, l'Union européenne prévoit que le transfert des données à caractère personnel vers un pays tiers n'est possible que dans les hypothèses listées par le Règlement Général sur la Protection des Données (RGPD).

Cependant, le RGPD n'est pas un outil de protection ayant une valeur contraignante pour tous les pays du monde. Dès lors, imposer son respect aux sociétés importatrices et exportatrices de données situées en dehors des frontières de l'Union européenne est un enjeu mondial complexe.

Et c'est notamment le transfert des données entre l'Union européenne et les Etats-Unis qui a fait grand bruit ces dernières années.

Après l'échec de deux traités entre l'Union européenne et les Etats-Unis, la présidente de la Commission européenne, Ursula Von Der Leyen, a annoncé en mars 2022 l'émergence d'un nouvel accord de principe dans l'espoir d'une nouvelle décision d'adéquation.

C'est donc avec beaucoup d'attente que l'Union européenne espère l'aboutissement d'une règlementation pérenne.

I- La nécessité d'un accord d'adéquation solide entre l'Union européenne et les Etats-Unis

Retour historique sur une relation internationale, le « Safe Harbor » fut le premier mécanisme d'adéquation permettant le transfert des données collectées par les entreprises vers les Etats-Unis. Ce traité a été annulé par la Cour de Justice de l'Union européenne (CJUE) le 6 octobre 2015 dans un arrêt Schrems I.

Une deuxième tentative a été intentée avec l'adoption du traité nommé « *Privacy Schield* », également annulé par la CJUE le 16 juillet 2020 dans un arrêt Schrems II.

L'heure d'une troisième tentative de mise en adéquation a donc sonné. La Commission européenne a communiqué certains points clés sur ce nouvel accord.

L'idée principale étant l'émergence de nouvelles règles afin de **limiter l'accès aux données des services de renseignements américains** comme le craint la CJUE.

Également, est évoqué l'idée d'un **recours** à deux niveaux pour permettre aux individus qui s'estiment lésés dans la collecte qui a été fait de leurs données de pouvoir obtenir une réparation.

Les particuliers pourront agir auprès d'un officier chargé de la protection des libertés civiles à la direction du renseignement américain, et, ils pourront ensuite faire appel de cette décision devant la « *Data Protection Review Court* » qui aura un pouvoir coercitif.

L'idée en stand-by depuis ces deux échecs est celle de permettre une libre circulation des données en toute sécurité.

En ce sens, la présidente de la Commission évoque un nouvel accord « *efficace* » qui assure « *le juste équilibre entre sécurité, d'une part, et droit à la vie privée et protection des données, d'autre part* ».

Dans le même ordre d'idée, le CEPD (Comité européen de la protection des données) évoque « *un engagement sans précédent de la part des Etats-Unis* » et « *une économie numérique inclusive à laquelle tous peuvent participer* ».

Les Etats-Unis, tout comme l'Union européenne semblent l'un comme l'autre faire preuve d'une volonté sans failles dans l'élaboration de ce nouveau projet d'adéquation. Pourtant, l'activiste autrichien Max Schrems, à l'origine des deux premières invalidations par la CJUE, craint déjà que la politique soit encore placée au-dessus des droits et des libertés fondamentales des individus.

Pourtant, bien qu'ils y travaillent activement, les Etats-Unis n'ont pas de réglementation comparable au RGPD dans leur système. De plus, la vision européenne diffère radicalement de la vision américaine en matière de

gestion des données. Là où l'Union perçoit la vie privée comme un droit fondamental où chacun est propriétaire de ses données, les entreprises américaines considèrent être propriétaires des données qu'elles collectent.

Google, géant de l'internet, qui a récemment communiqué à ce sujet, semble favorable à l'arrivée de ce nouvel accord.

On le comprend aisément dans la mesure où une plainte avait été déposée à son encontre par l'ONG « NOYB » auprès de la CNIL (Commission nationale de l'informatique et des libertés). La plainte portait sur le transfert des données européennes vers les Etats-Unis par le biais de Google Analytics, considéré comme non-conforme à la réglementation européenne.

Après expertise, la CNIL avait reconnu dans une décision du 22 décembre 2021 que l'usage de Google Analytics violait le RGPD.

Ce nouvel accord, s'il est adopté, pourra donc permettre aux entreprises d'utiliser de nouveau Google Analytics et notamment sa quatrième et dernière version, qui n'est, pour l'heure, que partiellement conforme au RGPD, et par conséquent non recommandable en l'état.

Mais alors, en attendant l'aboutissement de cet accord d'adéquation, quel comportement doivent adopter les entreprises pour encadrer efficacement le transfert des données de leurs utilisateurs ?

II- Une vigilance nécessaire des entreprises dans la protection des données

Pour rappel, le RGPD s'applique à toute entreprise disposant d'employés ou qui réalise des prestations ou vend des produits dans l'un des 27 états membres de l'UE. Cette réglementation impacte également toute entreprise exerçant une activité en ligne sur internet avec notamment l'exploitation d'un site web accessible aux citoyens de l'Union européenne.

La mise en conformité au RGPD des entreprises s'impose au surplus pour une société où le transfert des données avec les Etats-Unis est important.

Pour cela, le RGPD prévoit des exceptions dans lesquelles un transfert de données vers un pays tiers est admis.

C'est le cas lorsqu'une décision d'adéquation a été prise à l'égard du pays tiers par la Commission européenne qui considère alors la législation du pays en question adéquat à celle de l'Union. Décision toujours en attente pour le cas des Etats-Unis.

En parallèle, les entreprises peuvent aussi recourir aux clauses contractuelles types (CCT). Ce sont des modèles de clauses fournies par la Commission européenne et qui encadrent le transfert de données vers un pays tiers. Ces clauses ont été mises à jour par la Commission le 4 juin 2022 et ont désormais une approche par module en fonction de la qualité des parties au transfert (entre responsable de traitement et/ou sous-traitant).

Ces nouvelles clauses font suite à la jurisprudence Schrems II de la CJUE qu'elles intègrent pleinement. En effet, il est imposé à l'exportateur de données de prendre en compte la législation qui s'applique à l'importateur.

Le transfert des données dépendra alors non seulement des clauses contractuelles types, mais également des mesures supplémentaires mises en place par l'entreprise. A défaut, l'entreprise devra renoncer au transfert des données vers les Etats-Unis si l'ensemble de ses mesures ne permettent pas une protection suffisante.

Un dernier point peut permettre le transfert. Il s'agit du mécanisme des BCR (Binding Corporate Rules). Ces règles d'entreprise contraignantes permettent d'être en conformité avec les principes du RGPD selon la CNIL. Ces règles vont venir uniformiser les pratiques au sein d'un groupe international de sociétés et permettre de communiquer sur la politique du groupe. La CNIL indique en ce sens que le recours aux BCR permet de placer la protection des données « *au rang des préoccupations éthiques du groupe* » afin d'assurer un niveau de protection suffisant.

Enfin, la CNIL établit des **recommandations** sur le comportement que doivent adopter les entreprises ayant recours aux transferts internationaux de données personnelles.

En premier lieu, l'entreprise doit évaluer la législation du pays tiers dans lequel sont transférées les données et, au surplus mettre en œuvre des mesures supplémentaires pour que les données soient suffisamment protégées.

Mais c'est surtout dans l'information des personnes concernées par les transferts de données que réside tout l'enjeu juridique de la réglementation.

La transparence est une notion essentielle à respecter pour assurer un traitement des données conforme.

Le RGPD poursuit un objectif de sécurisation des données, mais aussi de responsabilisation des entreprises. Pour cela, il impose une obligation de transparence.

Cette obligation de transparence va permettre aux individus de savoir pourquoi leurs données personnelles sont collectées, mais aussi de comprendre comment le traitement va être effectué.

Ainsi, en respectant cette obligation, les entreprises pourront instaurer une relation de confiance avec les individus ayant recours à leurs services.

Malgré tout, l'urgence se fait ressentir auprès des entreprises lassées par la complexité qu'impose le transfert des données entre un pays de l'Union européenne et les Etats-Unis.

Suite à l'accord qui a été trouvé avec Bruxelles, le 7 octobre 2022, Joe Biden a signé un décret afin d'accélérer le cadre de ce nouvel accord. Mais malgré l'excitation, celui-ci ne devrait pas arriver avant l'été 2023. Les entreprises vont donc encore devoir s'armer d'un peu de patience.

En attendant, il est recommandé aux entreprises de privilégier les prestataires européens, ou pour le moins, d'héberger les données collectées sur le sol européen.

Lorsqu'une entité a recours au transfert de données personnelles, il convient également de faire preuve de transparence auprès des individus concernés. Pour cela, ces derniers doivent pouvoir être informé de manière claire sur le processus de traitement de leurs données dans la politique de confidentialité de l'entreprise ou dans les conditions générales de vente ou d'utilisation.

Le chiffrage et le cryptage des données personnelles des utilisateurs sont aussi des moyens permettant une protection des données. De tels procédés permettent de rendre les données confidentielles en les dotant d'un code, et seule la personne disposant d'un mot de passe pourra y avoir accès.

Quelque soit donc l'issue de ce projet, relatif aux transferts des données personnelles entre les deux puissances économiques, les entreprises se doivent d'être vigilantes et de se doter de tous les moyens existants permettant un transfert sécurisé des données en dehors des frontières de l'UE.

Ludovic de la Monneraye
Vaughan Avocats