Le bras de fer se poursuit entre l'Europe et les États-Unis : *Meta Platforms* infligé d'une amende historique de 1,2 milliard d'euros pour ses transferts de données personnelles vers les États-Unis

Aurelie Banck est Compliance Director d'Europcar Mobility Group qu'elle a rejoint en juin 2019. Elle est en charge de la définition et de l'implémentation du programme de conformité du Groupe couvrant trois domaines stratégiques : la protection des données personnelles, la lutte contre la corruption (notamment dans le cadre de la loi Sapin 2) et le devoir de vigilance. Disposant d'une expérience de plus de 16 ans en protection des données et conformité, elle est l'auteur de différents ouvrages. Elle est notamment diplômée du DU Responsable Conformité de l'Université Panthéon Assas et certifiée CIPP/E, CIPM et FIP.

Quelle est votre opinion sur la décision de l'autorité irlandaise de protection des données d'infliger une amende de 1,2 milliard d'euros à *Meta Platforms Ireland Limited* pour ses transferts de données personnelles vers les États-Unis *via* des clauses contractuelles types (CCT) ?

Je vous propose tout d'abord de revenir sur le contexte de cette sanction. Le contentieux tranché par l'autorité irlandaise de protection des données le 22 mai est l'aboutissement d'une plainte déposée par Max Schrems, il y a trois ans. Dans cette plainte, Schrems reproche à *Meta* de ne pas avoir adopter des mesures suffisantes pour protéger ses données personnelles dans le cadre de leur transfert vers les US en substituant, en tant qu'outil de transfert, des clauses contractuelles en lieu et place de la protection offerte par le *Privacy Shield* à la suite de l'invalidation de celui-ci par la Cour de Justice de l'Union Européenne en juin 2020. *Meta* comme d'autres entreprises à mis en place un nouvel outil de transfert pour sécuriser des flux à l'intention des US, pays tiers, c'est-à-dire ne présentant pas un niveau de protection équivalent ou similaire à celui offert au sein de l'Union européenne.

Ce qu'il faut également souligner c'est que ce contentieux a donné lieu à la mise en œuvre du mécanisme de règlement des litiges entre autorités de protection des données, mécanisme prévu par l'article 65 du RGPD et supervisé par l'*European Data Protection Board* (EDPB/CEPD)[1]. Cette décision ne reflète donc pas uniquement la position de l'autorité irlandaise mais également celle des autres autorités de protection des données qui ont obtenu des modifications substantielles de la proposition irlandaise, en particulier l'ajout de la sanction financière qui n'avait pas été proposée par l'autorité irlandaise initialement.

Elle n'est pas très surprenante au fond – ce qui peut l'être c'est le montant – qualifié par tous d'amende record dans la mesure où il s'agit du plus important prononcé dans le cadre d'une violation du RGPD – mais également sa sévérité à l'égard de *Meta* qui fait face à un problème structurel – à savoir l'invalidation du *Privacy Shield*. D'ailleurs, le caractère punitif de la sanction est mentionné dans la décision de l'EDPB à plusieurs reprises.

Quelles sont les principales raisons qui ont conduit à cette amende record ?

Tout d'abord, il convient de préciser que l'amende n'est qu'une partie de la sanction. L'autorité a également ordonné à *Meta* de suspendre les futurs transferts vers les US dans un délai de 5 mois à compter de la date de notification de la décision et de mettre en conformité les traitements de données transférées dans un délai de 6 mois. Donc la décision va au-delà de l'amende en tant que telle.

Pour résumer cette problématique complexe, certaines dispositions législatives aux États-Unis en particulier le FISA permettent à des autorités publiques d'accéder à des données personnelles d'une manière relativement extensive. L'utilisation de clauses contractuelles types en cas de transferts de données à destination d'un pays tiers vise à prolonger la protection offerte en Europe dans ce pays tiers. Ces clauses lient l'importateur et l'exportateur de données et ne sont pas opposables à un tiers comme les agences de renseignement américaines. Pour prévenir un risque d'atteinte à la vie privée des personnes, les exportateurs de données doivent mettre en place des garanties additionnelles après avoir procédé à une analyse de risques également appelée *Transfert Impact Assessment*[2]. Les mesures mises en place par *Méta* ont été jugées insuffisantes. *Meta* est donc sanctionné sur cette base.

Comment cette décision peut-elle avoir un impact sur d'autres entreprises qui effectuent des transferts de données similaires ?

Il faut noter c'est que l'Autorité irlandaise s'est prononcée sur les anciennes clauses contractuelles types applicables au moment de la plainte de Max Schrems mais également sur les nouvelles publiées le 4 juin 2021[3].

1 - Le Comité européen de la protection des données (CEPD) a rendu sa décision le 13 avril 2023 - Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR) | European Data Protection Board (europa.eu)
2 - Voir les recommandations de l'EDPB 01/2020 : EDPB_Recommendations_202001(Vo.2.0)_FR.docx (europa.eu)
3 - EUR-Lex - 32021D0914 - FR - EUR-Lex (europa.eu)

L'Autorité a non seulement considéré que les mesures additionnelles prises pas *Meta* n'étaient pas suffisantes pour réduire le risque d'accès par des autorités étrangères à des données personnelles aux US mais elle semble également remettre en cause cette approche adoptée par le CEPD dans ces recommandations (§7.27 et §7.28 de la décision). À ce stade, ce point n'est pas très clair et mérite des analyses approfondies.

L'Autorité a également analysé la possibilité d'utiliser les exceptions en tant qu'outil de transferts alternatifs, elle a donc interprété également ces dispositions.

En termes d'impact, cette décision va au-delà des transferts UE-US, dans la mesure où cet exercice doit être fait à chaque fois que des données sont transférées à l'intention d'un pays tiers.

Quelles sont les implications de cette amende pour la protection des données personnelles des utilisateurs de *Facebook* en Europe ?

Meta a annoncé faire appel de la décision en particulier pour suspendre l'application des délais[4]. *Meta* avait déjà menacé d'arrêter de fournir son service de réseau social en Europe, c'est une déclaration assez courante des acteurs américains face à la régulation européenne[5].

Donc à ce stade, je ne suis pas sûre que cette décision ait impact concret pour les utilisateurs de *Meta* en Europe.

Quelles mesures concrètes *Meta Platforms Ireland Limited* doit-elle prendre pour se conformer au RGPD en ce qui concerne ses transferts de données ?

C'est là toute la difficulté – à part, arrêter de procéder à des transferts et localiser les données en Europe, il apparaît très difficile d'identifier des mesures additionnelles que Meta pourrait mettre en œuvre. Par ailleurs, cela n'empêcherait pas l'application extraterritoriale de certaines réglementations américaines, *Meta* restant en particulier soumis au FISA[6].

Une autre solution serait que la loi américaine elle-même soit modifiée afin d'encadrer les accès aux données de la part d'autorités publiques. C'est ce qui pourrait résulter du nouvel *executive order* adopté par Joe Biden le 7 octobre 2022.

Comment cette décision peut-elle affecter les relations commerciales entre les entreprises européennes et les entreprises américaines qui traitent des données personnelles ?

Je ne suis pas sûre que cette décision ait un impact sur les relations commerciales tout du moins à ce stade ; ce que l'on a pu constater depuis *Schrems 2*, c'est le développement d'offres dites de *Cloud* souverain ou de confiance en Europe (offre Bleu de *Capgemini* et *Orange* par exemple) et une méfiance généralisée à l'égard des transferts de données à destination des US[7].

Existe-t-il d'autres mesures que les entreprises peuvent prendre pour se conformer aux exigences du RGPD concernant les transferts de données internationaux ?

Revoir les *transferts impacts assessments* et réévaluer les mesures additionnelles qu'elles ont déjà mis en place. Elles peuvent également envisager de changer d'outils de transferts pour substituer aux SCC l'une des exceptions, il apparaît cependant que ces exceptions ne peuvent pas être utilisées pour des transferts massifs et répétitifs.

Pensez-vous que cette amende incitera d'autres autorités de protection des données en Europe à prendre des mesures similaires à l'égard d'autres entreprises ?

C'est déjà le cas. Les récentes décisions portant sur l'utilisation de *Google Analystics* sont basées en tout ou partie sur une problématique de transferts de données. À noter également que l'Autorité belge de protection des données a également prononcée le 24 mai 2023 une sanction à l'égard du Service Public fédéral (SPF) finances de l'État belge dans le contexte de l'application de l'accord FATCA et portant également sur une question de transferts aux US.

Quels enseignements les entreprises peuvent-elles tirer de cette affaire pour éviter de se retrouver dans une situation similaire ?

Meta ayant mis en œuvre des mesures additionnelles en nombre, il semble difficile d'identifier des mesures additionnelles à mettre en place, à l'exception de mesures d'anonymisation des données ce qui par ailleurs aurait pour effet d'exclure l'application du RGPD. Les entreprises doivent s'interroger sur leur soumission au FISA et garder un œil sur le futur cadre de protection des données.

Quelles sont les prochaines étapes à suivre pour la conformité aux réglementations sur la protection des données en Europe, en particulier en ce qui concerne les transferts de données internationaux ?

Il y a quelques mois Joe Biden a signé l'*executive order* 14086[8] pour mieux encadrer les pratiques des agences de renseignement et permettre la mise en place d'un nouvel accord relatifs aux transferts, le cadre de protection des données « *UE US privacy framework* ». Cet accord est actuellement en cours d'analyse par la Commission européen. Il a donné lieu à un avis mitigé de l'EDPB le 28 février 2023[9] et à une résolution du Parlement européen le 11 mai 2023[10]. Bien que non-contraignante, cette résolution « *invite la Commission à ne pas adopter le*

4 - Voir le communiqué de Meta : Our Response to the Decision on Facebook's EU-US Data Transfers | Meta (ampproject.org)
5 - Le fondateur d'Open AI Sam Altman vient de faire la même déclaration à propos du futur règlement sur l'intelligence artificiel OpenAI menace de "cesser ses activités" en Europe en raison de la réglementation sur l'IA - ZDNet
6 - Foreign Intelligence Surveillance Act
7 - Décision quant au fond 61/2023 du 24 mai 2023 : decision-quant-au-fond-n-61-2023.pdf (autoriteprotectiondonnees.be)
8 - Federal Register : Enhancing Safeguards for United States Signals Intelligence Activities
9 - Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, edpb_opinion52023_eu-us_dpf_en.pdf (europa.eu)
10 - P9_TA(2023)0204 Adéquation de la protection assurée par le cadre de protection des données UE-États-Unis