Données personnelles, manque de transparence et contournement législatif : nouvelles sanctions record pour Meta

Description

Depuis l'entrée en vigueur du RGPD en 2018, la barre symbolique des 2 milliards d'euros de sanctions à l'encontre de Meta a été franchie.

Le 25 novembre 2022, la Data Protection Commission (DPC – Commission de protection des données en Irlande) a infligé une amende record de 265 millions d'euros à Meta Platforms Ireland Limited (filiale de Meta, maison mère de Facebook), pour violation de l'article 25 du règlement général sur la protection des données (RGPD)[1], pour défaillances de paramétrage par défaut et du traitement des données personnelles. La tendance étant à la sanction systématique des violations du RGPD, notamment pour non-conformité des méthodes de traitement des données à caractère personnel, cette sanction sera suivie d'une autre prononcée le 4 janvier 2023 d'un montant encore plus significatif de 390 millions d'euros : 210 millions d'euros pour Facebook et 180 millions d'euros pour Instagram pour défaut de base légale quant au traitement des données. Cette amende est assortie, en outre, d'une sommation de remise en conformité dans un délai de trois mois. Le cumul de ces deux amendes à l'encontre du groupe Meta fait écho à celle déjà infligée à Instagram le 2 septembre 2022 d'un montant de 405 millions d'euros pour manquements au traitement des données personnelles des mineurs et à celles qui sanctionnent également WhatsApp le 20 août 2021, s'élevant à 225 millions d'euros et le 19 janvier 2023, à hauteur de 5,5 millions d'euros pour manquements aux obligations d'information et de transparence relatives au traitement des données personnelles en vue de l'amélioration des conditions de sécurité des services.

265 millions d'euros pour les défaillances dans le paramétrage par défaut du traitement des données personnelles

En avril 2021, les médias ont rapporté qu'un ensemble de données personnelles de quelque 533 millions d'utilisateurs de Facebook ont été mises à disposition sur internet, à la suite d'un piratage de données liées aux fonctionnalités Facebook Search, Facebook Contact Importer, Messenger Contact Importer et Instagram Contact Importer, ci-après nommées les « fonctionnalités pertinentes »[2]. La DPC a estimé qu'il était nécessaire de déterminer si, sur la période allant de mai 2018 à septembre 2019[3], le groupe Meta s'était conformé à ses obligations relatives au traitement des données personnelles des utilisateurs, découlant du RGPD et/ou du Data Protection Act de 2018[4].

En effet, le système, tel que conçu initialement, a permis le recoupement de plusieurs types de données provenant de sources différentes (Facebook, Messenger…), grâce auxquelles les utilisateurs de faux comptes, pirates et *bots*[5], ont pu reconstituer un répertoire permettant d'identifier les utilisateurs réels. La

DPC a constaté que cette absence de garde-fous techniques a rendu possible ce piratage. Elle considère que ce manquement constitue une violation de l'article 25(1) du RGPD, lu en même temps que l'article 5(1), points b et f, relatifs aux principes de limitation des finalités de traitement des données à caractère personnel ainsi qu'aux principes d'intégrité et de confidentialité.

Par ailleurs, deux défaillances ont été identifiées quant au traitement des données par Meta. Premièrement, les paramètres de recherche par défaut étaient programmés de façon à inclure automatiquement le numéro de téléphone et l'adresse électronique de chaque utilisateur. Cet automatisme nécessitait l'intervention de l'utilisateur afin de le désactiver. Deuxièmement, il a été constaté que lorsqu'un utilisateur ajoutait son numéro de téléphone pour effectuer l'authentification à double facteur (A2F), cette action rendait automatiquement le numéro de téléphone consultable dans les « fonctionnalités pertinentes », et les utilisateurs se retrouvaient là encore tenus de modifier les paramètres de leur téléphone pour empêcher que leur numéro soit visible. Tous les utilisateurs ayant indiqué leur numéro de téléphone à des fins d'A2F étaient repérés par défaut et soumis à la fonctionnalité de recherche inversée.

En conséquence, les données des utilisateurs ont été mises à disposition des pirates et de leurs *bots* grâce à cette fonctionnalité de recherche inversée. Et les profils Facebook ont également été rendus consultables *via* les fonctionnalités pertinentes, quand bien même leurs titulaires n'avaient pas fourni de numéro de téléphone à des fins de recherche. La DPC a en ce sens considéré que Meta n'avait pas correctement mis en œuvre les mesures techniques et organisationnelles appropriées afin de garantir par défaut que seules les données à caractère personnel nécessaires à chaque finalité spécifique du traitement soient traitées, enfreignant ainsi l'article 25(2) du RGPD qui prévoit cette restriction. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. Par défaut, les données à caractère personnel ne doivent pas être rendues accessibles à l'insu de la personne concernée.

Il en résulte que la DPC a infligé une sanction pécuniaire à Meta pour la violation de l'article 25(1) du RGPD, en lui imposant de plus, s'agissant de la violation de l'article 25(2) du RGPD, de mettre en œuvre les mesures nécessaires à son respect. Les amendes de 150 millions d'euros pour la violation de l'article 25(1) et de 115 millions d'euros pour la violation de l'article 25(2) s'accompagnent donc de la lourde sommation à prendre des mesures de remise en conformité dans un délai de trois mois, sanction pouvant se révéler la plus coûteuse du fait des interventions et opérations à déployer.

390 et 405 millions d'euros pour la seule violation de l'article 6 du RGPD

L'association de défense de la vie privée Noyb (None Of Your Business) a déposé une plainte le 25 mai 2018, le jour de l'entrée en vigueur du RGPD, remettant en cause le fondement juridique utilisé par Meta pour son service Facebook, en vue de légitimer le traitement des données personnelles à des fins publicitaires [6]. Il était reproché à la plateforme, d'une part, la publication des adresses de courrier électronique et des numéros de téléphone des personnes mineures ayant un compte Instagram professionnel, et d'autre part le paramétrage « public » par défaut qui rend visibles les données des comptes personnels. Ceci résulte d'une

réinterprétation de la notion de consentement comme contrat de droit civil applicable à la plupart des opérations de traitement des données personnelles. Par conséquent, le choix de cette base légale pour le paramétrage par défaut imposait la publicité ciblée, sans possibilité de la refuser. Partant, si les utilisateurs souhaitaient avoir accès aux services de Facebook et d'Instagram, ou continuer d'y avoir accès, ceux-ci devaient accepter les conditions de service, à défaut de quoi l'accès leur était refusé.

Dans son projet de décision, la DPC avait initialement envisagé de valider la base juridique retenue, et d'infliger une amende allant de 26 à 36 millions d'euros pour défaut de transparence. Mais la Cnil (Commission nationale de l'informatique et des libertés) et d'autres régulateurs nationaux européens ont contesté cette position estimée trop légère et mal fondée. En effet, la DPC était d'avis que les services proposés par Facebook et Instagram comprenaient, par essence, un service personnalisé nécessitant la mise en place de publicités ciblées ou personnalisées. Dès lors, il était considéré que ceci constituait un des points essentiels des contrats conclus entre les utilisateurs et les fournisseurs de services Facebook et Instagram. Les différentes autorités de contrôle ont tenté de trouver un consensus sur ce point litigieux. En vain.

Face à ces objections et désaccords, la DPC s'en est remise au Comité européen de la protection des données (CEPD), afin de trancher le différend qui les opposait en adoptant une décision contraignante, conformément à l'article 65 du RGPD[7]. Le 5 décembre 2022, le CEPD a validé la considération de la DPC selon laquelle le groupe Meta avait manqué à son obligation de transparence, sous réserve d'y ajouter la mention de la « violation du principe d'équité », et en demandant d'augmenter le montant des sanctions[8]. Concernant l'autre point, et contrairement à ce qu'avait initialement proposé la DPC, le CEPD rejette la considération selon laquelle Meta pouvait utiliser la base juridique de l'article 6 du RGPD relative au « contrat », à des fins de publicité personnalisée. Le CEPD a ainsi conclu que Meta ne pouvait s'appuyer sur le fondement de l'article 6(1)(b), en ce que la publication des adresses de courrier électronique et des numéros de téléphone des mineurs qui utilisaient des comptes professionnels n'était pas nécessaire à l'exécution d'un contrat entre l'utilisateur et la plateforme[9]. Conformément au caractère contraignant des décisions du CEPD, la DPC se voit ordonnée de prendre en compte, dans sa décision finale du 4 janvier 2023, le fait que Meta a violé l'article 6 du RGPD, et condamne l'entreprise à une amende de 390 millions d'euros.

Cela fait écho à la retentissante décision du 2 septembre 2022[10], par laquelle la DPC a infligé une amende de 405 millions d'euros à Instagram pour violation de ses obligations de transparence concernant le traitement des données à caractère personnel des mineurs. Ici encore, la base légale avancée par la filiale de Meta applicable à la publication de ces données était l'objet du litige. Instagram justifiait déjà la nécessité de publication des données des personnes mineures pour l'exécution du contrat selon l'article 6(1)(b) du RGPD, ainsi que l'intérêt légitime selon l'article 6(1)(f) du RGPD. Prête à admettre le fondement juridique avancé, la DPC fait l'objet de critiques virulentes de la part des autorités de contrôle nationales, ce qui aboutit à la saisine du CEPD. Faisant suite à la décision contraignante adoptée par celui-ci le 28 juillet 2022 [11], la DPC a infligé 20 millions d'euros pour la seule violation de l'article 6 RGPD, compris dans l'amende globale de 405 millions d'euros, en ce que la publication des données des personnes mineures n'était ni nécessaire à l'exécution d'un contrat, ni ne présentait un intérêt légitime. Ces amendes record ont donc pour

objectif, selon les instructions du CEPD, d'exercer une pression persuasive et suivie d'effets pour la mise en conformité avec le RGPD, tout en maintenant l'application du principe de proportionnalité dans la mise en œuvre de ces sanctions.

Facebook, Instagram, puis WhatsApp, vers des sanctions à une cadence soutenue

La messagerie instantanée WhatsApp, une autre branche du groupe Meta, s'était vu infliger une amende de 225 millions d'euros le 20 août 2021, pour manquement aux obligations d'information et de transparence. WhatsApp était accusée, par non moins de quatre-vingt-huit plaintes émanant de différentes autorités de contrôle nationales, de transférer les données des utilisateurs à d'autres entreprises liées à Meta (à l'époque, Facebook), constituant ainsi un défaut de transparence. Ayant eu accès à des données personnelles de non-utilisateurs de la plateforme *via* les conversations enregistrées de ses utilisateurs, WhatsApp a failli à ses obligations d'information et de transparence, quant à l'exercice des droits des personnes concernées[12]. L'utilisation et le transfert des données n'étant pas les seuls manquements en cause, la DPC a infligé le 19 janvier 2023 une amende supplémentaire de 5,5 millions d'euros à WhatsApp pour avoir, de nouveau, failli à son obligation de transparence, et pour s'être fondée sur une base juridique erronée pour la collecte et le traitement de données personnelles, supposément *« en vue de l'amélioration des conditions et de la sécurité du service »*[13]. Ce défaut de transparence et d'information tout comme la violation de l'article 6 du RGPD montrent la volonté de Meta de contourner la législation européenne.

Or, il est également apparent que l'Union européenne ne cessera de poursuivre ces manquements et violations, quand bien même le faible montant de cette dernière amende de 5,5 millions d'euros semble déstabiliser la lancée répressive et dissuasive contre le géant américain. Il faudra donc attendre d'éventuelles prochaines condamnations pour entériner ce constat, tout en notant la barre symbolique des 2 milliards d'euros de sanctions à l'encontre de Meta franchie depuis l'entrée en vigueur du RGPD en 2018.

Les opinions exprimées dans le présent article ne reflètent que celles de l'auteur et n'engagent pas la Cour de justice de l'Union européenne.

Sources :

1. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ; texte présentant de l'intérêt pour l'Espace économique européen, JO 2016 L 119/1.
2. Les « fonctionnalités pertinentes » (traduction de *relevant features*) font référence à l'ensemble des outils Facebook Contact Importer, Messenger Contact Importer, Instagram Contact Importer, Messenger Search et sa variante Messenger Contact Creator. Voir le point 44 de la décision de la DPC du 25 novembre 2022, IN-21-4-2.
3. Un incident similaire avait déjà eu lieu en 2019, où les données de 419 millions d'utilisateurs avaient

été rendues publiques et accessibles en ligne, résultant d'une faille que Meta (alors Facebook) a déclaré avoir réparé à cette époque.

4. Data Protection Bill 2018 (Bill 10 of 2018).
5. Robot ou agent autonome artificiel utilisé sur les plateformes informatiques comme interface de dialogue avec des serveurs informatiques. Ces robots, dits *« bots »*, peuvent être programmés pour une utilisation malveillante telle que la collecte, la reconstitution et la diffusion des données.
6. Pour rappel, selon l'article 6 du RGPD, « le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie : a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ; b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ; c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ; d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ; e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ; f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant ».
7. Le CEPD est composé des chefs des autorités de contrôle de chaque État membre, ou leurs représentants, ainsi que du contrôleur européen de la protection des données, ou de ses représentants. Dans le cas présent, il adopte des décisions contraignantes afin de résoudre un différend entre des autorités de contrôle nationales (article 65 RGPD), quand bien même il peut être sollicité à titre consultatif afin d'émettre des avis (article 64 RGPD) ou des orientations générales afin d'éclairer les droits et obligations découlant de la législation européenne (article 70 RGPD).
8. Voir « Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (art. 65 GDPR) », edpb.europa.eu, December 5, 2022, points 482 et s.
9. Voir le communiqué de presse de la Cnil du 15 septembre 2022, cnil.fr.
10. Décision de la DPC du 2 septembre 2022, IN-20-7-4.
11. « Binding Decision 2/2022 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR », edpb.europa.eu, September 15, 2022.
12. Voir « Une consécration du mécanisme européen de contrôle de la cohérence ? À propos de la décision WhatsApp Ireland Limited de l'autorité de contrôle irlandaise du 20 août 2021 », Jérôme Deroulez, *La Semaine du droit*, édition générale, n° 41, 11 octobre 2021.
13. Voir le communiqué de presse de la DPC du 19 janvier 2023, dataprotection.ie/en/news-media.

Categorie

1. Droit

date créée
7 juin 2023
Auteur
abihanna