

---

## ACTUALITÉS NOVEMBRE-DÉCEMBRE 2021

---

### 1. Partage de données au sein des pays de l'Union Européenne : un texte à venir

Le Conseil de l'Union Européenne s'est récemment positionné sur le futur « Data Governance Act » qui a vocation à « réguler la gouvernance des données » au sein de l'Union Européenne. Ce texte, proposé par la Commission Européenne en novembre 2020, s'inscrit dans une perspective d'un marché unique de données, l'objectif étant de promouvoir la disponibilité des données et « de créer un environnement fiable pour faciliter leur utilisation à des fins de recherche et de création de nouveaux services et produits innovants ».

Il permettrait ainsi à l'Union Européenne de se doter d'un cadre permettant de fournir un environnement sécurisé pour le partage de données.

Du côté des particuliers, les législateurs européens ont insisté sur le fait qu'il permettra aux citoyens de disposer d'un contrôle total sur leurs données, et de choisir de les partager ou non avec l'/les entreprise(s) en qui ils ont confiance.

Récemment, le Parlement européen et le Conseil de l'Union Européenne se sont accordés sur les conditions de la mise en œuvre du texte. Néanmoins, il s'agit pour l'instant d'un accord provisoire.

### 2. Évolution de loi relative à la protection des données : Loi Québécoise

Le Gouvernement Québécois a récemment fait évoluer sa loi relative à la protection des données notamment pour la rapprocher des dispositions du Règlement Européen à la Protection des Données (RGPD).

Le texte impose, entre autres, aux sociétés de réaliser des études d'impact sur la vie privée pour les transferts de données effectués hors du Québec, de désigner des agents chargés de la protection des données et d'aviser les personnes concernées en cas de violation des données lorsqu'il existe un risque de préjudice grave (cette dernière obligation étant imposée à l'ensemble des sociétés relevant de la compétence de la loi Québécoise). Des pouvoirs pour prononcer des amendes administratives sont également attribués à l'Autorité Québécoise de protection des données. Il est prévu que le montant de celles-ci puisse atteindre 10 millions de dollars canadien ou 2% du chiffre d'affaires mondial de l'année précédente d'une entité. Les manquements constitutifs d'infraction pénale pourront être sanctionnés d'une amende de 25 millions de dollars canadiens ou d'une amende équivalente à 4% du chiffre d'affaires mondial.

La plupart des dispositions seront applicables à compter du mois de septembre 2023, les autres entreront en vigueur en 2022 ou pour certaines en 2024.

### 3. Décisions rendues par la CEDH

#### ➤ **Violation de la liberté d'expression reconnue sur le fondement de l'article 10 de la CEDH (CEDH, 7 décembre 2021, Case of Standard Verlagsgesellschaft mbh c. Autriche)**

L'affaire concernait des décisions de justice ayant ordonné au média Standard Verlagsgesellschaft mbh de révéler les données d'inscription d'utilisateurs ayant déposé des commentaires sur le site web de son journal Der Standard.

Lesdits commentaires auraient associé certaines figures politiques du pays à la corruption et au mouvement néonazi.

Le journal, dont le site était soumis à une modération partielle, avait alors retiré les commentaires litigieux mais avait refusé de divulguer les informations sur leurs auteurs. En effet, le journal disposait de leur nom et adresse email voire, si renseignée, de leur adresse postale, étant précisé qu'il indiquait aux utilisateurs que ces informations ne seraient pas visibles des autres internautes et ne seraient divulguées qu'en cas d'obligation résultant de la loi.

Dans le cadre de son arrêt\*, la Cour a jugé que « *les données d'utilisateurs ne sont pas couvertes par la protection des « sources journalistiques » et qu'il n'y a pas de droit absolu à l'anonymat en ligne* ». Elle retient que les commentaires s'adressaient au public et non à un journaliste.

En revanche, elle a retenu que la fonction générale du média était de « *favoriser un débat ouvert et de diffuser des idées sur des questions d'intérêt public, mission protégée par la liberté de la presse* », de même « *une obligation de divulguer les données d'utilisateur est de nature à avoir un effet dissuasif sur la participation au débat* ».

Ainsi, elle a jugé sur ce point que « *les juridictions nationales n'ont pas procédé à une mise en balance entre les intérêts des demandeurs en justice et les intérêts de la société requérante à maintenir l'anonymat de ses utilisateurs en vue de favoriser le libre échange des idées et des informations, protégé par l'article 10. Dès lors, les décisions judiciaires en question n'étaient pas nécessaires dans une société démocratique* ».

*\*Cet arrêt a été rendu par la chambre de la Cour et n'est donc pas définitif un renvoi devant la Grande chambre étant encore possible dans un délai de 3 mois.*

[Pour consulter l'arrêt et son résumé](#)

#### **4. Accès aux données de connexion : suite**

Le Conseil Constitutionnel du Pays voisin a, par décision en date du 3 décembre 2021, censuré plusieurs dispositions du code de procédure pénale autorisant la réquisition, par le procureur de la République, de données de connexion, dans le cadre d'une enquête préliminaire.

Ces dispositions ont été jugées contraires à la Constitution en raison de l'atteinte portée à la vie privée des personnes.

Cette décision fait suite au dépôt d'une Question Prioritaire de Constitutionnalité à travers laquelle les requérants estimaient notamment qu'un contrôle préalable d'une juridiction indépendante devrait être exigé.

A compter du 31 décembre 2022, une telle réquisition, dans le cadre d'une enquête préliminaire, ne pourra donc plus uniquement être décidée par le Procureur.

Ce délai a vocation à permettre au législateur de réformer l'accès aux données de connexion dans le cadre d'une enquête préliminaire (peut-être en tenant compte des dernières décisions rendues par la Cour de Justice de l'Union Européenne).

#### **5. Open Data des décisions de justice**

Un décret n° 2021-1276 daté du 30 septembre 2021 crée, dans le Pays voisin, deux traitements automatisés de données à caractère personnel directement liés à l'Open Data des décisions de justice.

Il s'agit d'un traitement mis en œuvre par le Conseil d'Etat intitulé « *Décisions de la justice administrative* » et d'un traitement mis en œuvre par la Cour de cassation intitulé « *Judilibre* ». Ces derniers ont pour finalité de diffuser, « éventuellement enrichies », les décisions de justice administratives et judiciaires, de conserver les données en vue d'une telle diffusion et de traiter les demandes d'occultation et de levée d'occultation.

Il est prévu que les jurisprudences soient ajoutées, tous les deux mois, sur une plateforme et classées dans des répertoires.

Certains points restent toutefois à adresser, comme a pu le relever le Conseil National des Barreaux français.

## 6. Enquêtes et sanctions prononcées par les autorités de contrôle européennes

### ➤ Europe

#### - Sur « *classement* » des CNIL européennes

Une étude a récemment permis d'analyser les pratiques des autorités de protection des données et de mettre en évidence celles ayant prononcé, jusqu'à présent, les amendes les plus importantes.

Il en ressort que l'autorité luxembourgeoise se classe en tête avec une amende d'un montant de 746 millions d'euros prononcée à l'encontre d'Amazon.

La CNIL arrive en seconde position après avoir sanctionné Google d'une amende de 50 millions d'euros pour insuffisance d'information des utilisateurs s'agissant de la collecte de leurs données et de leur utilisation dans le cadre de publicités ciblées.

Suivent l'Allemagne (amende de 35 millions d'euros à l'encontre d'H&M), l'Italie (27 millions d'euros à l'encontre de Gruppo ITM) et enfin le Royaume-Uni (22 millions d'euros et 20 millions à l'encontre de British Airways et Marriott).

S'agissant des autorités ayant quantitativement prononcé le plus d'amendes il appert que l'autorité espagnole a prononcé 273 amendes. Elle est suivie de l'Italie (75), la Roumanie (60), la Hongrie (43), la Norvège (31) et la Suède (26).

Concernant le *ratio* nombre d'amendes/montant, la constance des autorités italienne, allemande, française, britannique est ressortie de l'étude.

L'absence de base légale a motivé la plupart des sanctions prononcées : 276 d'entre elles. L'insuffisance de moyens techniques et organisationnels a engendré le prononcé de 155 amendes et les manquements aux principes généraux 149.

#### - Plateforme Vinted

Un groupe de travail a récemment été constitué entre les autorités de protection des données française, lituanienne et polonaise afin d'enquêter sur les pratiques de la plateforme Vinted après avoir reçu un grand nombre de plaintes.

L'attention de ces autorités a été portée sur la pratique consistant à demander aux utilisateurs une copie numérisée de leur carte d'identité pour débloquer le montant des transactions effectuées sur le compte de l'utilisateur. Sont également à l'étude les durées de conservation des données et la procédure et les critères pour bloquer un compte sur la plateforme.

### ➤ Irlande

Une plainte pénale pour corruption a été déposée à l'encontre de l'Autorité de protection des données irlandaise par l'ONG NOYB (*My Privacy is not Your Business* dont le fondateur est Maximilien Schrems).

Cette plainte s'inscrit dans le cadre du conflit opposant l'ONG à l'Autorité de protection irlandaise à propos de l'instruction de la plainte qu'elle a déposée à l'encontre de META (ex-Facebook).

NOYB lui reproche de l'avoir empêché de publier des documents liés aux procédures à laquelle elle est pourtant partie.

L'ONG estime à cet égard « être victime de *chantage procédural* » et réproouve le fait que l'autorité irlandaise ait tenté de lui imposer la signature d'un accord de non-divulgence

concernant la procédure qu'elle a engagée contre Facebook/Meta. A défaut de signature, il lui a été indiqué qu'elle serait exclue de la procédure.

Or, NOYB considère que cet accord ne repose sur aucune base juridique et qu'« *il s'agit d'un régulateur qui demande clairement une « contrepartie » pour faire son travail, ce qui constitue probablement un acte de corruption en Autriche* ».

Selon son fondateur, « *la DPC [l'autorité irlandaise] outrepassa d'une part le droit autrichien, mais également le droit irlandais selon lequel « les parties ne sont pas légalement tenues de garder les documents confidentiels »* ».

Il s'agit là d'une nouvelle critique portant sur la pratique de l'autorité irlandaise régulièrement remise en cause.

#### ➤ **Commission Européenne**

Dans le prolongement de ce qui précède, l'ONG Conseil Irlandais des Libertés Civiles (CILC) a déposé une plainte, à l'encontre de la Commission Européenne, devant le Médiateur européen.

Elle lui reproche d'une part, de ne pas avoir mis en place de mécanisme de surveillance de la bonne application du RGPD à Dublin et, d'autre part de ne pas avoir poursuivi l'Autorité de protection des données irlandaise.

Son représentant estime que « *Non seulement la Commission n'a pas agi, mais elle ne s'est même pas dotée des connaissances nécessaires pour prendre la décision d'agir* ».

L'ONG accuse également l'Autorité irlandaise de protection des données « *de freiner l'application du RGPD en Europe* ».

#### ➤ **France**

La CNIL a annoncé la réalisation de 42 contrôles effectués par ses services concernant les dispositifs mis en place par le Gouvernement pour lutter contre la COVID-19.

#### ➤ **Luxembourg**

Une enquête visant un organisme avait été ouverte, sous la forme d'un audit, en 2018 afin de vérifier la conformité de sa pratique avec la section 4 du Chapitre 4 du RGPD « *Délégué à la Protection des Données* ».

Il avait été relevé à cette occasion des manquements à l'obligation de désigner un délégué à la protection des données sur la base de ses qualités professionnelles, de l'associer à toutes les questions relatives à la protection des données, de lui fournir les ressources nécessaires et concernant ses contrôles.

L'autorité luxembourgeoise réunie en formation restreinte lui a infligé une amende d'un montant de 13.200 euros. (Pour plus d'informations la [Délibération 36FR/2021](#)).

#### ➤ **Belgique**

##### - **Plateforme vaccinale**

L'Autorité de protection des données belge a adressé un courrier à la Cocom (Commission Communautaire Commune) pour solliciter des informations complémentaires concernant la sécurité des données sur la plateforme vaccinale Bruvax. Elle demande, entre autres, comment les services juridiques ont évalué le niveau de sécurité pour estimer qu'il n'y avait pas de failles dans le système et, à quel moment la Cocom a été alertée d'une fuite potentielle de données.

##### - **Bannière cookie**

L'International Advertising Bureau (IAB) Europe (organisation réunissant les acteurs de la publicité numérique) avait annoncé le 5 novembre dernier qu'elle s'attendait à être reconnue coupable de non-conformité au RGPD par l'autorité belge de la protection des données agissant en qualité d'autorité chef de file (art. 56 1) du RGPD).

Une plainte avait en effet été déposée à l'encontre de cette organisation en raison de la conception « *des fenêtres pop-up trompeuses de « consentement » qui figure sur la quasi-totalité des sites web et applications européennes (Transparency & Consent framework) »*. IAB a indiqué qu'elle ne s'était jusqu'à présent pas considérée comme étant un responsable de traitement s'agissant du « *Transparency & Consent framework* » qu'elle développe. Un projet de décision vient d'être partagé par l'autorité belge avec les autres autorités européennes de protection des données concernées.  
A suivre.

*Commission de Contrôle des Informations Nominatives*  
*Ce document est à vocation purement informative et ne peut être considéré comme reflétant une position officielle de la CCIN*