Actualités
Novembre-Décembre 2022

1. Avancements en faveur d'un nouvel encadrement des transferts de données UE-USA

Plus de deux années après l'invalidation du *Privacy Shield*[1] par la Cour de Justice de l'Union européenne (CJUE), la Commission européenne a lancé, le 13 décembre dernier, une procédure destinée à aboutir à un nouvel accord. En effet, depuis juillet 2020, les transferts outre-Atlantique doivent faire l'objet d'un encadrement et de garanties supplémentaires appropriées pour empêcher tout accès par les autorités américaines de renseignement aux données transférées. Pour rappel, la décision de la CJUE avait été motivée en raison de l'état de la législation américaine en matière de surveillance (Section 702 FISA et Executive Order 12 333).

Au mois de mars dernier, la présidente de la Commission européenne, Madame Von der Leyen, a annoncé qu'un accord de principe avait été trouvé en faveur d' « *un nouveau cadre pour les flux de données transatlantiques* ». En octobre dernier, le Président américain a signé en ce sens un décret visant à protéger les données transférées aux Etats-Unis (*Executive Order 14086*) à l'égard duquel le Commissaire à la justice, Monsieur Didier Reynders, a pu souligner l'existence de garanties solides *« désormais en place aux États-Unis pour permettre les transferts en toute sécurité de données à caractère personnel de part et d'autre de l'Atlantique* ».

Du point de vue de l'association NYOB, dont le fondateur Max Schrems a été à l'origine de l'invalidation du Safe Harbor puis du Privacy Shield, les évolutions apportées au texte américain seraient minimes, de sorte que ce dernier ne répondrait toujours pas aux attentes de la CJUE en raison de l'existence d'une surveillance massive continue et de l'absence de véritable tribunal compétent pour connaître des recours judiciaires. Partant, le nouvel accord entre l'Union européenne et les Etats-Unis pour encadrer la protection des données serait voué à un échec.

Le projet de texte est présentement soumis à l'avis du Comité européen à la protection des données. Un texte définitif n'est pas attendu avant le printemps 2023.

2. Retour sur l'échec de la vente du fichier clients de Camaïeu

Dans le prolongement de la liquidation judiciaire de Camaïeu, une vente aux enchères des derniers actifs (notamment immatériels) de l'enseigne a eu lieu le 7 décembre. Cette dernière devait initialement comprendre, parmi les lots proposés à la vente, le fichier clients regroupant l'ensemble des détenteurs d'une carte fidélité. Ce fichier contenait près de 4 millions de clients et comprenait notamment leur identité, leurs adresses, emails, numéros de téléphone, etc...

Pourtant attendu, le lot en question n'a toutefois pas été mis à la vente « *par précaution* », « *compte tenu des risques juridiques encourus* » au titre du Règlement général sur la protection des données et, plus particulièrement, des règles encadrant la cession de fichiers clients.

L'Autorité de protection des données française (CNIL) en a profité pour rappeler les principes encadrant la vente de fichiers clients. A cet égard, elle a souligné que si la vente d'un fichier clients, y compris lors d'une vente aux enchères, n'est pas interdite par le RGPD, celle-ci doit se faire dans le respect du cadre légal. Elle a rappelé ainsi que « *le* vendeur *doit s'assurer que la base de données ne contienne que les clients « actifs »*, «*de ne pas envoyer les données des clients qui ne souhaitaient pas qu'elles soient transmises à des tiers soit parce que les clients s'y sont opposés (pour la transmission des données à des fins de prospection par voie postale ou téléphonique) soit parce qu'ils n'ont pas consenti (pour la transmission des données à des fins de prospection par voie électronique)* » ».

[1] Le Privacy Shield constituait le cadre législatif qui encadrait le transfert de données entre les Etats-Unis et l'Union européenne

3. Autorités de protection des données et autres Autorités

- Autriche

Intérêt légitime d'un avocat au traitement de données dans le cadre d'une procédure judiciaire

L'Autorité de protection des données autrichienne s'est prononcée sur la légitimité d'un avocat à traiter les données personnelles d'un tiers dans le cadre d'une procédure judiciaire.

En l'espèce, l'avocat d'une société Y avait obtenu les données d'un plaignant par le biais de sa cliente qui les avait, elle-même, récupéré dans le cadre d'un échange au sein d'un groupe d'entreprises par l'intermédiaire d'une société X.

Le plaignant contestait l'utilisation de ses données personnelles par l'avocat d'une société avec laquelle il était en conflit. Le plaignant estimait que son droit à la confidentialité des données avait été lésé, la société X n'étant pas en droit de transmettre ses données personnelles à la société Y et donc à son avocat. Il soulignait à cet égard qu'un tel transfert n'était pas prévu par la politique de confidentialité et qu'il n'y avait pas consenti.

L'Autorité de protection des données autrichienne devait dès lors se prononcer sur la possibilité pour un avocat de traiter, au nom de sa cliente, les données d'un plaignant dans le cadre d'une procédure civile initiée par ce dernier.

L'Autorité a rappelé en premier lieu que le droit à la confidentialité des données n'est pas un droit absolu et qu'un traitement peut se justifier par la préservation des intérêts prépondérants d'autrui. Elle a, en outre, rappelé que les avocats agissent régulièrement en qualité de responsable de traitement lorsqu'ils traitent des données dans le cadre de leur mission de représentation de leurs clients. De plus, l'article 9 paragraphe 2 f) du RGPD rend possible l'utilisation de données particulières, même contre la volonté d'une personne, dans le cadre d'une procédure judiciaire, cette base pouvant également être utilisée pour justifier une atteinte au droit au secret.

- Belgique

Mise en garde d'un employeur n'ayant pas procédé à l'effacement des photos et des informations concernant le poste d'un ancien salarié sur son site internet

Une personne avait indiqué à son ancien employeur qu'elle ne souhaitait désormais plus figurer sur le site internet de la société (6 mois après son licenciement). En effet, une photo de l'ancien employé, accompagnée de l'intitulé de son ancien poste et une photo où elle était représentée au sein d'un groupe d'autres salariés, demeuraient sur ledit site. En l'absence de réponse de l'employeur, l'ancien salarié avait adressé une plainte à l'Autorité de protection des données.

Cette dernière a considéré que la finalité du traitement n'était plus valide à la suite du licenciement du salarié puisque l'objectif d'une telle publication est d'informer les internautes sur les personnes travaillant au sein d'une entreprise et sur leur fonction. Aussi, de telles données auraient dû être supprimées ou anonymisées dès lors qu'elles n'étaient plus nécessaires à cette finalité (sauf à ce qu'elles soient nécessaires pour une autre finalité conforme au RGPD). L'Autorité a par ailleurs considéré que lorsqu'un salarié quitte son poste, le responsable de traitement doit s'efforcer de retirer le plus rapidement possible de son site/page de réseau social les informations relatives à l'identité, la fonction, la/les photographies de la personne concernée, quelques semaines ou un mois maximum étant des délais suffisants pour cela. De même, l'Autorité belge a souligné qu'une procédure devrait être mise en place pour le départ de salariés mais également pour traiter les questions en lien avec la protection des données, étant précisé que si un responsable du traitement n'efface pas de

telles données de sa propre initiative, il doit réagir dans les meilleurs délais dès lors qu'il reçoit une demande en ce sens. Le délai d'effacement peut quant à lui varier en fonction de plusieurs facteurs (ex. : la taille du responsable de traitement, la nature des fonctions occupées par la personne, le contexte de son départ, etc.).

Mise en garde d'un responsable de traitement ayant procédé à la publication d'une facture contenant des données personnelles sur Facebook

Un fournisseur de services (responsable de traitement) avait publié sur sa page Facebook une facture contenant les nom, prénom et adresse d'un client avec lequel il était apparemment en conflit. A la suite d'une plainte déposée par le client concerné, auprès des autorités de police locales, le responsable de traitement avait procédé à l'effacement de l'adresse du plaignant, tout en conservant son nom et son prénom. Le nom et le prénom de ce dernier étaient par ailleurs apparents dans certains commentaires présents sur la page. Dans le même temps, le responsable de traitement avait bloqué le plaignant, l'empêchant d'accéder à la page Facebook sur laquelle restait publiée la facture.

Partant, le plaignant s'est rapproché de l'Autorité de protection des données belge. Si cette dernière a rappelé que l'établissement d'une facture nécessite la collecte de certaines informations par le responsable de traitement (nom, prénom, adresse de facturation, adresse de livraison, adresse électronique), elle a néanmoins considéré que la publication de la facture litigieuse comportant les nom et prénom de la personne concernée ne remplissait aucune des conditions de licéité du traitement prévues à l'article 6 du RGPD, notamment l'intérêt légitime du responsable de traitement qu'il ne pouvait, en l'espèce, invoquer.

- <u>France</u>

Microsoft Ireland Operations Limited: dépôt de cookies

La formation restreinte de l'Autorité de protection des données française (CNIL) a infligé à Microsoft Ireland Operations Limited une amende de près de 60 millions d'euros pour n'avoir pas mis en place un mécanisme permettant de refuser le dépôt de cookies aussi facilement que pour les accepter. Cette amende a été assortie d'une injonction de corriger cette pratique dans un délai de 3 mois. A défaut, la société sera tenue de payer une astreinte de 60 000 euros par jour de retard.

Il y a lieu de relever que la CNIL a déjà prononcé des sanctions en ce sens par le passé.

En l'espèce, elle avait été saisie de plaintes d'utilisateurs visant les conditions du dépôt de cookies sur le moteur « bing.com ». A l'issue des contrôles effectués, l'autorité a constaté que « *lorsqu'un utilisateur se rendait sur ce site, des cookies étaient déposés sur son terminal sans consentement de sa part alors qu'ils poursuivaient, notamment, un objectif publicitaire. Elle a également constaté l'absence d'un bouton permettant de refuser le dépôt de cookies aussi facilement que de l'accepter* ». Sur ce dernier point, il est apparu que deux clics étaient nécessaires pour refuser les cookies contre un pour les accepter.

Sanction d'une plateforme pour non-suppression de comptes d'utilisateurs inactifs

La CNIL a par ailleurs sanctionné pour non-respect du Règlement général sur la protection des données une plateforme d'une amende de 800 000 euros. Il lui était notamment reproché la non-suppression des comptes des utilisateurs inactifs. En outre, l'Autorité a retenu que le responsable de traitement ne disposait pas d'une politique claire en matière de conservation des données de ses utilisateurs.

Amende infligée à FREE MOBILE

L'opérateur FREE MOBILE a été sanctionné d'une amende de 300 000 euros pour non-respect des droits des personnes et de la sécurité des données de ses utilisateurs. Cette

sanction fait suite à la réception de plusieurs plaintes par la CNIL, lesquelles ont donné lieu à des contrôles sur place et sur pièces.
Ainsi, sur le volet relatif au non-respect des droits des personnes, l'autorité de protection des données a relevé que l'opérateur n'avait pas respecté le droit d'accès des personnes à leurs données et ne leur avait pas donné la possibilité de procéder à l'effacement de celles-ci.
Par ailleurs, en termes de manquements à la sécurité des données, elle a notamment constaté une faible robustesse des mots de passe générés automatiquement par le site web lors de la création d'un compte ou d'une procédure de récupération. En outre, ces derniers étaient stockés « *en clair* » dans la base des abonnés de la société. En toute fin, il a été reproché à l'opérateur de n'avoir pas protégé les données de ses abonnés dès la conception, ces derniers continuant de recevoir des factures téléphoniques pour des lignes dont l'abonnement avait pourtant été résilié.

Manquements d'EDF
Le producteur et fournisseur d'électricité EDF doit s'acquitter d'une amende de 600 000 euros en raison de plusieurs manquements au RGPD. Il lui est, entre autres, reproché de ne pas avoir recueilli le consentement des personnes pour recevoir de la prospection commerciale par voie électronique lors de sa campagne réalisée entre 2020 et 2021. En outre, des manquements à l'obligation d'information et au respect de l'exercice des droits des personnes ont été relevés. Ainsi, *« la charte de protection des données personnelles qui figurait sur le site web de la société ne précisait pas la base légale correspondant à chaque cas d'usage des données et était imprécise sur les durées de conservation* ». Enfin, des faiblesses en matière de sécurité des données (conservation non-sécurisée de mots de passe d'accès à un espace client de près de 25 000 comptes) ont également été observées.

- Espagne

Droit d'accès
L'autorité catalane de protection des données s'est prononcée sur une problématique relative au droit d'accès à un dossier d'enquête menée par une administration publique.
En l'espèce, les parents d'un élève, dont il était supposé qu'il fût victime de harcèlement scolaire, avaient demandé, à l'établissement scolaire (responsable de traitement), d'accéder au dossier de l'enquête qui avait été menée. L'établissement leur avait toutefois refusé cet accès au motif que le dossier contenait des données personnelles concernant d'autres élèves et leurs parents, le personnel de l'établissement ainsi que d'autres données sensibles. Les parents déposaient dès lors une plainte auprès de la Commission pour la garantie du droit d'accès à l'information publique laquelle a saisi, pour avis, l'autorité catalane de protection des données.
Cette dernière, après, s'être prononcée sur la base légale du traitement, a considéré que les informations relatives à la présomption de harcèlement devaient être considérées comme étant publiques, l'enquête étant effectuée par une administration publique (l'établissement). En outre, les parents du mineur possiblement victime des agissements litigieux étaient en droit d'accéder aux informations en leur qualité de représentant légal du mineur. Concernant plus précisément l'étendue du droit d'accès, après avoir analysé les dispositions de la Loi régionale sur la transparence et l'accès à l'information publique et mis en balance les intérêts en présence, l'autorité a autorisé l'accès aux documents relatifs à la personne concernée ; aux données d'identification des employés publics impliqués dans l'enquête ; aux données d'identification des employés impliqués ; et aux noms, prénoms et déclarations de tiers, à moins que l'audition préliminaire ne démontre une justification pour limiter leur identification.

- Grèce

Absence de mise en place de mesures techniques et organisationnelles
L'opérateur de téléphonie mobile Vodafone PANAFON SA a écopé d'une amende de 150 000 euros pour absence de mise en place de mesures techniques et organisationnelles.
L'autorité de protection des données hellénique avait été saisie de plaintes d'usagers reprochant notamment à l'opérateur des remplacements non autorisés de leurs cartes SIM, des déviations d'appels ou encore des changements de cartes SIM au profit de tiers non autorisés dont il prétendait qu'un contrôle d'identité avait été effectué pour écarter tout comportement frauduleux.
A l'issue des vérifications effectuées, l'autorité de protection des données a rappelé qu'en qualité de responsable de traitement, il revenait à l'opérateur de démontrer qu'il traitait les données de manière licite et transparente et dans le respect des principes d'intégrité et de confidentialité. Elle a également rappelé, qu'en application de la loi transposant la directive e-privacy, le responsable de traitement est tenu de prendre des mesures techniques et organisationnelles appropriées pour protéger la sécurité de ses services et du réseau public de communications électroniques. Or, elle a estimé que le responsable de traitement n'avait, en l'espèce, pas mis en œuvre de politiques de sécurité suffisantes dans le processus de remplacement des cartes SIM pour prévenir des fraudes et ce en dépit des mesures supplémentaires adoptées par l'opérateur après les premiers incidents. Enfin, l'autorité a considéré que les personnes concernées n'avaient pas été informées des violations de leurs données de manière conforme à l'article 12 du RGPD, l'opérateur les ayant informés deux à trois mois après et non sans délai.

Autres autorités

- Cour européenne des droits de l'homme (CEDH) (Affaire Drelon c. France)

La Cour européenne des droits de l'homme a été saisie, en vertu de l'article 34 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, de deux requêtes dirigées contre la France. Ces requêtes concernaient notamment la collecte et la conservation de données personnelles permettant de refléter l'orientation sexuelle d'un des requérants.
Ce dernier avait en effet tenté à plusieurs reprises d'effectuer un don du sang auprès de l'Etablissement français du sang (EFS). Au cours d'un premier entretien médical préalable effectué auprès d'un des établissements de l'EFS, il lui avait été demandé s'il avait déjà eu un rapport sexuel avec une personne de même sexe. Refusant de répondre, sa candidature avait été rejetée. Par la même occasion, certaines de ses données avaient été saisies dans un fichier informatique propre à l'établissement (son nom, ses coordonnées). En outre, il fût renseigné, dans ce traitement de données, comme personne contre-indiquée au don du sang sous le code FR08, lequel correspondait à cette époque à celui prévu pour les hommes ayant eu un rapport sexuel avec un autre homme. Ce code était propre à l'établissement lié à l'EFS.
Deux ans plus tard, il avait tenté de renouveler sa démarche et avait été exclu au motif qu'il était référencé sous le code FR08.
Après avoir sollicité un extrait des données le concernant, le requérant constatait que la contre-indication avait inscrite à son dossier et que l'interdiction était valable jusqu'en 2278.
Dix ans plus tard, il réitérait de nouveau sa démarche en présentant cette fois-ci des analyses de sang attestant de sa séronégativité au VIH-1, au VIH-2 et au VHC. Sa candidature était pourtant une fois de plus rejetée en raison de pratiques homosexuelles supposées.
Le requérant avait donc fini par initier des procédures en France puis, avait saisi la CEDH.

Cette dernière a considéré que l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales consacrant le droit à la vie privée avait été méconnu par l'EFS à l'occasion de la collecte et de la conservation des données concernant le requérant et qu'il y avait eu une ingérence non proportionnée dans le droit au respect de la vie privée de ce dernier.

A cet effet, la Cour a notamment retenu qu' « *eu égard à la sensibilité des données personnelles litigieuses, qui comportent des indications sur les pratiques et l'orientation sexuelles du requérant, (…) il est particulièrement important qu'elles répondent aux exigences de qualité prévues à l'article 5 de la Convention de 1981. Il importe en particulier qu'elles soient exactes et, le cas échéant, mises à jour, qu'elles soient adéquates, pertinentes et non excessives par rapport aux finalités du traitement, et que leur durée de conservation n'excède pas celle qui est nécessaire. Par ailleurs, la Cour constate que les données litigieuses, qui touchaient à l'intimité du requérant, ont été collectées et conservées sans le consentement explicite du requérant – ce que le Gouvernement défendeur ne conteste pas. En conséquence, elle se doit de procéder à cet examen de façon rigoureuse* ». Ainsi, s'agissant de l'exactitude des données personnelles, elle a estimé que « *celle-ci doit être appréciée au regard de la finalité pour laquelle ces données ont été collectées. Dans le traitement litigieux, cette catégorie de données avait pour finalité d'assurer le respect d'une contre-indication au don spécifique, que le droit interne prévoyait alors de façon permanente. À cette fin, elle devait reposer sur une base factuelle précise et exacte. Or, le requérant s'est vu appliquer une contre-indication propre aux hommes ayant eu un rapport sexuel avec un homme au seul motif qu'il avait refusé de répondre à des questions relatives à sa sexualité lors de l'entretien médical préalable au don. Aucun des éléments soumis à l'appréciation du médecin ne lui permettait de tirer une telle conclusion sur ses pratiques sexuelles. C'est pourtant ce motif d'exclusion du don qui fut renseigné et conservé. La Cour en déduit que les données collectées se fondaient sur de simples spéculations et ne reposaient sur aucune base factuelle avérée. Or, la Cour rappelle que c'est aux autorités qu'il incombe de démontrer l'exactitude des données collectées. Elle relève de surcroît qu'elles n'ont pas avoir été mises à jour à la suite des protestations et de la plainte du requérant*. Enfin, concernant la durée de conservation des informations litigieuses, la Cour a considéré que « *le Gouvernement ne démontre pas qu'à l'époque des faits, la durée de conservation des données litigieuses était encadrée de telle sorte qu'elle ne puisse pas excéder celle nécessaire aux finalités pour lesquelles elles ont été collectées. La Cour note qu'au moment de la collecte de ces données en 2004, l'outil informatique employé par l'EFS prévoyait leur conservation jusqu'en 2278*, *rendant ainsi possible leur utilisation de manière répétée. À la date du 26 mai 2016, soit près de douze ans après leur collecte, les données relatives au motif d'exclusion étaient encore conservées. À cet égard, la Cour tient à souligner que la durée de conservation des données doit être encadrée pour chacune des catégories de données concernées et qu'elle doit être révisée si les finalités pour lesquelles elles ont été collectées ont évolué. La Cour relève, au vu de la pratique constante de l'EFS, que la durée excessive de conservation des données litigieuses a rendu possible leur utilisation répétée à l'encontre du requérant, entraînant son exclusion automatique du don de sang* ».

Pour plus d'informations : cliquez ici

- Conférence allemande sur la protection des données (« *Datenschutzkonferenz* »)

D'après le résultat d'un groupe de travail, mené dans le cadre de la Conférence allemande sur la protection des données, dévoilé le 25 novembre dernier, le service Cloud Microsoft 365 ne serait pas conforme au Règlement européen sur la protection des données. Ce groupe de travail, lancé au début de l'automne 2020, était constitué de l'Autorité fédérale de protection des données et d'autorités de protection de plusieurs Länder avec également une participation de l'entreprise américaine. Cette dernière a d'ailleurs mis à jour deux ans plus tard ses contrats sans que cela ne soit toutefois suffisant.

En effet, au terme du rapport rendu, il est reproché à Microsoft « *le flou de ses formulations* », ne permettant pas de savoir en détail comment sont traitées les données. Il en est de même s'agissant des données que Microsoft estime pouvoir garder légitimement pour ses propres activités. Des incertitudes auxquelles l'avenant de septembre 2022 ne permet pas de répondre demeurent notamment s'agissant de la politique de conservation et de suppression des données. Enfin, la question du transfert des données dans le contexte de l'invalidation du Privacy Shield en 2020 a été abordée, le rapport mettant en avant l'impossible fonctionnement de Microsoft 365 sans un transfert de données vers les Etats-Unis. De même, le groupe a estimé qu'il était impossible pour l'entreprise de crypter les données.
De son côté l'entreprise a indiqué « *être respectueusement en désaccord avec les préoccupations soulevées par la Datenschutzkonferenz* » et a rappelé avoir collaboré avec cette dernière.

- Comité européen à la protection des données (CEPD)

Le 6 décembre dernier, 3 décisions contraignantes ont été adoptées par le CEPD. Ces décisions concernent Facebook, Instagram et WhatsApp et « *répondent à des questions juridiques importantes sur des projets de décisions de l'autorité de protection des données irlandaise en qualité d'autorité de chef de file* ». La saisine du CEPD, institué par le Règlement européen sur la protection des données (RGPD), dont la mission principale est de veiller à la bonne application du règlement par les autorités de protection nationales, fait suite au désaccord de plusieurs autorités s'agissant de l'analyse retenue par l'autorité irlandaise dans son projet de décision. Ces désaccords porteraient notamment sur la base légale du traitement retenue ainsi que sur les principes de protection des données et le recours à des mesures correctives.