NEWSLETTER RGPD/DATA

NUMÉRO 54 ● 2023

SOMMAIRE

FORMATION A LA PREPARATION A LA CERTIFICATION « DPO ».
DATE SUR DEMANDE

ET SI L'ANONYMISATION ETAIT (FINALEMENT) POSSIBLE ?

Le Tribunal de l'Union Européenne (TUE) a annulé une décision du CEPD qui recommandait au Conseil de Résolution Unique (CRU) de modifier sa « déclaration de confidentialité ».

Le Conseil de Résolution Unique (CRU) est un organe de l'Union Européenne ayant notamment pour rôle de minimiser les conséquences d'une faillite d'une banque sur l'économie réelle.

A l'occasion de la faillite d'une banque espagnole, le CRU a lancé une consultation sur son site internet afin de déterminer s'il fallait, ou non, accorder un dédommagement aux actionnaires et créanciers de la banque qui s'est retrouvée insolvable.

Pour cela, les créanciers et actionnaires éligibles étaient invités à émettre des « *commentaires* », par la voie d'un formulaire, sur le site du CRU.

Pour procéder à l'examen des milliers de commentaires reçus, le CRU a fait appel au cabinet Deloitte : dans les faits, les commentaires transmis à Deloitte portaient un code alphanumérique unique. Au moyen de ce code, seul le CRU était en mesure de relier le commentaire à la personne l'ayant déposé.

Certaines personnes ayant déposé des commentaires ont appris que les données collectées par CRU avaient été transmises à des tiers et ont déposé une plainte devant le CEPD.

Ce dernier a estimé que les données partagées avec Deloitte (i) « *étaient des données à caractère personnel* » et (ii) que « *Deloitte était un destinataire* » non mentionné dans la déclaration de confidentialité.

En conséquence, bien que n'adoptant pas de sanction à l'encontre du CRU, le CEPD a recommandé à ce dernier de modifier sa « *déclaration de confidentialité* ».

Le CRU a saisi le TUE aux fins d'annuler la décision du CEPD en considérant que « *les informations transmises à Deloitte ne constituent pas des données à caractère personnel* ».

Selon le TUE, une « *information constitue une donnée à caractère personnel […] si deux conditions cumulatives sont réunies, à savoir, d'une part, que cette information " se rapporte " à une personne physique et, d'autre part, que cette personne soit " identifiée ou identifiable "* ».

Le TUE a successivement analysé ces deux conditions.

I. L'information se rapporte à une personne physique

Le TUE s'est, dans un premier temps, penché sur la première condition. Selon lui, « s'*il ne saurait être exclu que des points de vue personnels ou des opinions constituent des données à caractère personnel […] une telle conclusion ne peut être fondée sur une présomption […] mais doit s'appuyer sur l'examen visant à déterminer si, par son contenu, sa finalité ou son effet, un point de vue est lié à une personne déterminée* ».

Constatant que le CEPD n'avait « *examiné ni le contenu, ni la finalité, ni l'effet des informations transmises à Deloitte* » et avait présumé que « *toute opinion personnelle constituait une donnée à caractère personnel* », le TUE a considéré qu'à « *défaut d'avoir procédé à un tel examen, le CEPD ne pouvait conclure que les informations transmises à Deloitte constituaient des informations " se rapportant " à une personne physique* ».

II. La personne est identifiée ou identifiable

Le TUE s'est, dans un second temps, penché sur la « *question de savoir si les informations transmises à Deloitte se rapportaient à une personne physique " identifiée ou identifiable "* ».

Le TUE a d'abord rappelé que « *les informations transmises à Deloitte ne concernaient pas des personnes " identifiées "* ».

En ce qui concerne le caractère « *identifiable* », le CRU, d'un côté, considérait que les données communiquées à Deloitte étaient « *anonymes* » *« dans la mesure où le CRU n'aurait pas partagé avec Deloitte les informations permettant de réidentifier les auteurs des commentaires* ». Inversement, le CEPD soutenait « *que le fait que Deloitte n'ait pas eu accès aux informations détenues par le CRU [n'avait] pas pour conséquence que les données " pseudonymisées " soient devenues des données anonymisées* ».

Pour répondre à cette problématique, le TUE a rappelé que pour « *déterminer si les informations transmises à Deloitte constituaient des données à caractère personnel […] il convient de se placer du point de vue de ce dernier* ».

Or, en présumant que les données transmises à Deloitte étaient des données à caractère personnel sur le seul fait que « *le CRU détenait les informations supplémentaires permettant de réidentifier les auteurs des commentaires* », le CEPD ne s'est pas placé du point de vue de Deloitte.

Plus encore, le TUE a considéré qu'à défaut « *pour le CEPD d'avoir recherché si Deloitte disposait de moyens légaux et réalisables en pratique lui permettant d'accéder aux informations supplémentaires nécessaires à la réidentification des auteurs des commentaires, le CEPD ne pouvait conclure que les informations transmises à Deloitte constituaient des informations se rapportant à une " personne physique identifiable " »*.

Compte tenu de ce qui précède, le TUE a annulé la décision du CEPD.

Source : CJUE 26 avril 2023 n° T-557/20, Conseil de résolution uniquement contre contrôleur européen de la protection des données

L'INSUFFISANCE DE CONFORMITE EST SANCTIONNEE AU MEME TITRE QUE L'INEXISTENCE DE CONFORMITE

Par une délibération du 11 mai 2023, la CNIL a prononcé une amende de 380 000 euros à l'encontre de Doctissimo, reprochant à cette dernière de nombreux manquements au RGPD.

La CNIL a été saisie d'une plainte par l'association Privacy International reprochant à l'éditeur du site internet doctissimo.fr un non-respect du RGPD.

A l'issue de son enquête sur pièce et sur place, la CNIL a notamment relevé plusieurs manquements :

I. Le manquement à l'obligation de conserver les données personnelles pour une durée n'excédant pas celle nécessaire au regard des finalités

La CNIL a d'abord constaté que le site conservait les réponses aux quizz des internautes pendant 24 mois. Cette durée était justifiée par Doctissimo pour permettre à l'internaute de connaître le résultat du quizz, pour partager ledit résultat et pour réaliser des statistiques sur l'utilisation du test.

Rappelant le principe de « *limitation de la conservation* », la CNIL, a considéré que Doctissimo violait l'article 5 du RGPD puisque (i) la conservation des données « *n'apparaît pas nécessaire après la communication du résultat à l'utilisateur et son éventuel partage par ce dernier à ses amis* », a tout le moins « *ces finalités ne sauraient […] justifier une conservation d'une durée de 24 mois* » et (ii) en ce qui concerne les statistiques, que « *la conservation des réponses au [quizz] après la fin du test n'était pas nécessaire* » pour cette finalité dès lors que d'autres outils de mesure d'audience (notamment les cookies) étaient présents.

Plus précisément, la CNIL a indiqué que, selon elle, la conservation des données relatives à la participation de l'utilisateur aux quizz « *n'apparaît pas nécessaire après la communication du résultat à l'utilisateur et son éventuel partage* » et que, même une « *durée de trois mois […] excède la durée nécessaire aux finalités pour lesquelles elles sont traitées* ».

La CNIL a également constaté que les données des comptes créés par les utilisateurs étaient anonymisées après 3 ans d'inactivité, mais a considéré que Doctissimo violait l'article 5 du RGPD dès lors que la procédure d'anonymisation des comptes *« ne correspondait pas à une anonymisation mais à une simple pseudonymisation »* puisqu'il était possible de réidentifier indirectement la personne.

II. Le manquement à l'obligation de recueillir le consentement des personnes concernées au traitement de catégories particulières de données

La CNIL a constaté que Doctissimo traite des données de santé lorsque les internautes répondent à des « *questionnaires ayant pour thème la santé* ».

Considérant qu'un tel traitement « *ne peut être mis en œuvre que sur la base du consentement explicite de la personne concernée* », la CNIL a constaté qu' « *aucun avertissement particulier ni mécanisme de recueil du consentement ne figurait sur les questionnaires* » et a considéré que Doctissimo a manqué aux obligations de l'article 9 du RGPD.

III. Le manquement à l'obligation d'assurer la sécurité des données

La CNIL a constaté que le site internet utilisait (i) le protocole de communication HTTP et (ii) l'algorithme de hachage MD5.

Rappelant les recommandations de l'ANSSI et de la CNIL, cette dernière a considéré (i) que le passage au protocole HTTPS était une « *précaution élémentaire* » et (ii) que l'algorithme MD5 devait être considéré comme « *définitivement cassé* », et dont « *l'utilisation en cryptographie ou en sécurité est à proscrire* ». En conséquence, la CNIL a considéré que Doctissimo avait manqué à l'article 32 du RGPD en méconnaissant les mesures de sécurité élémentaires.

IV. Le manquement aux obligations de la loi « Informatique et Libertés »

La CNIL a constaté que des cookies ayant pour finalité la « *publicité ciblée* » étaient déposés sur le terminal des internautes « *dès [leur] arrivée sur la page d'accueil du site* », « *avant que leur consentement ne soit recueilli* ». De même, certains cookies ayant la même finalité étaient déposés « *malgré le refus exprimé par l'utilisateur* ».

Rappelant le principe selon lequel, sauf si le cookie permet ou facilite « *la communication par voie électronique* » ou est « *strictement nécessaires à la fourniture d'un service* », le dépôt et l'accès aux cookies suppose le consentement de l'internaute, et constatant que le refus du dépôt de cookies était privé d'effet, la CNIL a considéré que Doctissimo a violé l'article 82 de la loi Informatique et Libertés.

Compte tenu de tout ce qui précède, la CNIL, a infligé à Doctissimo (i) une amende de 280 000 euros pour non-respect des articles 5, 9, 26 et 32 du RGPD et (ii) une amende de 100 000 euros pour non-respect de l'article 82 de la loi Informatique et Libertés.

Source : ici

IA ET DONNEES PERSONNELLES : LA CNIL PUBLIE SA FEUILLE DE ROUTE SUR LES IA GENERATIVES

La protection des données personnelles est un enjeu majeur pour l'ensemble des concepteurs et utilisateurs des systèmes d'IA.

Après avoir annoncé la création d'un service dédié à l'IA début janvier, la Cnil a publié le 16 mai 2023, un plan d'actions pour un déploiement des systèmes d'IA respectueux de la vie privée des individus.

Un plan d'action qui fait clairement écho au développement massif des IA génératives de texte (Chat-GPT, Bard), d'images (Stable Diffusion, Midhourney, Dall-E…) ou de voix.

Ce plan d'actions se décompose en « *quatre volets :*

- *appréhender le fonctionnement des systèmes d'IA et leurs impacts pour les personnes ;*
- *permettre et encadrer le développement d'IA respectueuses des données personnelles ;*
- *fédérer et accompagner les acteurs innovants de l'écosystème IA en France et en Europe ;*
- *auditer et contrôler les systèmes d'IA et protéger les personnes* ».

Dans ce cadre, la Cnil renvoie aux recommandations publiées courant 2022 et annonce la publication prochaine d'un guide sur les règles applicables au partage et à la réutilisation de données, et à partir de l'été 2023 de recommandations sur la conception de systèmes d'IA et la constitution de bases de données pour l'apprentissage automatique.

Le Laboratoire d'innovation numérique de la CNIL (LINC) a par ailleurs publié un dossier consacré aux IA génératives qui notamment :

- expose différentes questions juridiques posées par la conception de ces modèles, tant en matière de protection des données que sur d'autres enjeux come la propriété intellectuelle ;

- précise les enjeux éthiques des IA génératives pour la fiabilité de l'information, les utilisations malveillantes ainsi que les pistes de détection et avertissement du public quant à la présence de contenus générés.

Source : ici

CJUE : LE DROIT D'ACCES ET LA REMISE DE DOCUMENTS

Dans un arrêt du 4 mai 2023, la Cour de justice de l'Union européenne (CJUE) a indiqué que, pour répondre de façon satisfaisante à une requête au titre du droit d'accès au sens du RGPD, il peut être nécessaire d'adresser à la personne concernée la copie d'extraits de documents, voire de documents entiers.

Un individu a exercé son droit d'accès auprès d'une société, dont l'activité consiste à fournir à ses clients des informations concernant la solvabilité de tiers. Par cette demande, l'individu a expressément sollicité la fourniture d'une copie des documents contenant ses données personnelles, notamment des courriers électroniques et des extraits de bases de données.

La société a transmis à la personne concernée, pour toute réponse, la liste des données à caractère personnel faisant l'objet du traitement, sous forme de tableau synthétique.

Estimant que la société aurait dû lui transmettre une copie des documents contenant ses données personnelles, la personne concernée a introduit une réclamation auprès de l'autorité autrichienne de protection des données. Cette dernière a rejeté la réclamation, considérant que la société avait correctement répondu, sans enfreindre les règles en matière de droit d'accès.

La personne concernée a exercé un recours contre cette décision de rejet, auprès du tribunal administratif fédéral d'Autriche. Cette juridiction a posé une série de questions préjudicielles à la CJUE, afin de déterminer si l'obligation de donner suite à une demande de droit d'accès impliquait « *de transmettre des extraits des documents, voire des documents entiers, ainsi que des extraits de bases de données, dans lesquels ces données sont reproduites* ».

Par son arrêt du 4 mai 2023, la CJUE apporte les réponses suivantes :

- L'objectif poursuivi par le droit d'accès est de permettre à la personne concernée de s'assurer que les données à caractère personnel la concernant sont exactes et qu'elles sont traitées de manière licite.

- Le droit d'accès suppose « *celui d'obtenir la copie d'extraits de documents voire de documents entiers ou encore d'extraits de bases de données qui contiennent, entre autres, lesdites données, si la fourniture d'une telle copie est indispensable pour permettre à la personne concernée d'exercer effectivement les droits qui lui sont conférés par ce règlement, étant souligné qu'il doit être tenu compte, à cet égard, des droits et libertés d'autrui.* »

Source : ici

LE RAPPORT D'ACTIVITE 2022 DE LA CNIL

Comme chaque année, la CNIL a publié un rapport retraçant son activité au cours de l'année écoulée, soit, en l'occurrence, 2022.

En préambule de son rapport d'activité, publié le 23 mai 2023, la Présidente de la CNIL indique que 2022 marque « *la fin d'un cycle au cours duquel la CNIL a modifié ses méthodes de travail pour répondre aux exigences du RGPD, dans le domaine de l'accompagnement à la conformité et de l'information du public* ».

Pour ce qui est des chiffres, en 2022, la CNIL indique avoir traité 13 425 plaintes, ce qui est supérieur au nombre de plaintes reçues pour cette même année (12 193).

La CNIL a ainsi atteint, et dépassé, son objectif de traitement de 100% des plaintes. Certaines de ces plaintes, relatives aux exigences de l'arrêt « Schrems II », ont par ailleurs conduit la CNIL à mettre en demeure des organismes de ne plus utiliser l'outil Google Analytics, et a amené la CNIL à alerter les pouvoirs publics sur « *la nécessaire construction d'une souveraineté numérique européenne, notamment au travers du développement d'offres de solutions cloud immunisées contre l'extraterritorialité d'un droit étranger* ».

Sur le plan des contrôles, 345 ont été effectués, dont :

- 143 contrôles sur place ;
- 43 contrôles sur pièces ;
- 128 contrôles en ligne ;
- 31 contrôles sur audition.

Ces contrôles ont donné lieu à 147 mises en demeure et 21 sanctions, dont 19 amendes, représentant un montant cumulé de 101 277 900 euros.

Par ailleurs, au cours de l'année 2022, la CNIL annonce avoir été notifiée de 4 088 violations de données, contre 5 037 en 2021. Ces notifications arrivent par « vague » car un incident unique touchant un sous-traitant peut aboutir à autant de notification CNIL qu'il y a de responsables du traitement.

Ce rapport revient sur les différentes normes et décisions adoptées par la CNIL au cours de l'année 2022, à l'instar des référentiels destinés aux laboratoires pharmaceutiques concernant les accès précoces et les accès compassionnels.

Quant à ses projets en cours, enfin, la CNIL annonce notamment procéder à la mise à jour des méthodologies de référence MR-005 et MR-006.

Source : ici

TRANSFERTS DE DONNEES AUX ETATS-UNIS : META CONDAMNEE A UNE AMENDE RECORD DE 1,2 MILLIARDS D'EUROS

L'autorité de contrôle irlandaise a prononcé une amende d'1,2 milliards d'euros à l'encontre de Meta, pour avoir transféré des données personnelles aux Etats-Unis.

Pour rappel, le 16 juillet 2020, la CJUE a rendu un arrêt « *Schrems 2* » par lequel elle a invalidé le « *Privacy Shield* » et a fortement restreint les possibilités de transférer des données personnelles aux Etats-Unis. Cette décision était motivée par les captations larges et intrusives de données personnelles opérées par les autorités américaines.

En Aout 2020, la DPC (« *Data Protection Commission* », autorité de protection irlandaise) a entamé une enquête spontanée à l'égard de Meta Ireland, dont l'objet était de s'assurer de la conformité des transferts de données personnelles vers Meta US, située aux Etats-Unis, dans le contexte de la fourniture des services liés à Facebook.

1. Les clauses contractuelles types

La DPC a relevé que les transferts de données personnelles réalisés par Meta Ireland à destination des Etats-Unis étaient couverts, successivement, par les clauses contractuelles types version 2010, puis version 2021.

Sans surprise, pour la DPC, les clauses contractuelles types, quelle que soit leur version, ne lient pas les autorités américaines et, en conséquence, ne permettent pas d'assurer, à elles seules, la conformité des transferts de données personnelles aux Etats-Unis.

2. Les « *mesures supplémentaires* »

Meta Ireland et Meta US avaient mis en œuvre les « *mesures supplémentaires* » suivantes :

- Des mesures d'ordre organisationnel, composées d'un certain nombre de politiques et de procédures implémentées chez Meta Ireland et Meta US, par lesquelles Meta US s'obligeait notamment à :
    - notifier à Meta Ireland tout réception d'une requête d'une autorité publique américaine, sauf prohibition de le faire en vertu de la loi ;
    - soumettre un rapport détaillé à Meta Ireland quant aux fournitures de données sur la base des requêtes américaines.

- Des mesures d'ordre techniques, notamment par le chiffrement des données en transit ;

- Des mesures d'ordre légal, impliquant notamment l'obligation, pour Meta US, de former un recours contre les décisions émanant d'autorités américaines qu'elle estimait illégales, ou qui ne seraient pas nécessaires ou proportionnées dans une société démocratique.

Pour la DPC, aucune de ces mesures ne compense la protection inadéquate résultant de la loi américaine.

3. Le décret présidentiel du 7 octobre 2022

Il est à noter que, dans le cadre des débats entre la DPC et Meta Ireland, cette dernière a sollicité de la DPC qu'elle prenne en compte, dans le cadre de sa décision, les dispositions du décret présidentiel du 7 octobre 2022, dont l'objet est d'encadrer les pratiques de surveillance des autorités américaines, ainsi que fournir des moyens de recours aux citoyens européens.

Sur ce point, la DPC a noté que le décret présidentiel du 7 octobre 2022 n'oblige pas, de façon immédiate, les agences de renseignement américaines à changer leur pratique. Par ailleurs, le mécanisme de recours mentionné dans ce décret présidentiel n'est pas, à l'heure actuel, accessible aux citoyens européens. La DPC en a conclu que les risques identifiés par la CJUE dans sa décision « *Schrems 2* » étaient toujours d'actualité.

4. La sanction

Si l'intention initiale de la DPC n'était pas de prononcer une amende administrative à l'égard de Meta Ireland, mais uniquement d'ordonner la cessation du transfert, le CEPD a exprimé une volonté contraire, conduisant la DPC à assortir l'ordre de cessation des transferts, sous 5 mois, d'une amende administrative record d'1,2 milliards d'euros.

Source : ici

DOCTRINE

RGPD

L'application du principe de minimisation à un média

Comme chaque mois, Alexandre Fievée tente d'apporter des réponses aux questions que tout le monde se pose en matière de protection des données personnelles, en s'appuyant sur les décisions rendues par les autorités nationales de contrôle au niveau européen et les juridictions européennes. Ce mois-ci, il se penche sur la problématique de la licéité de la publication par un média d'un enregistrement audio de la déclaration faite devant un juge par une victime anonyme de viols.

Dans l'optique de concilier le droit à la protection des données et le droit à la liberté d'expression et d'information, les traitements de données personnelles aux fins de journalisme et d'expression littéraire et artistique bénéficient d'un régime dérogatoire.

Ainsi, l'article 85 du RGPD indique que : « *les États membres prévoient des exemptions ou des dérogations au chapitre II (principes), au chapitre III (droits de la personne concernée), au chapitre IV (responsable du traitement et sous-traitant), au chapitre V (transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales), au chapitre VI (autorités de contrôle indépendantes), au chapitre VII (coopération et cohérence) et au chapitre IX (situations particulières de traitement) si celles-ci sont nécessaires pour concilier le droit à la protection des données à caractère personnel et la liberté d'expression et d'information* ».

Dans ce cadre, le législateur français a considéré que, à titre dérogatoire, plusieurs articles du RGPD ne s'appliquent pas aux traitements de données personnelles réalisés à des fins de journalisme et d'expression littéraire et artistique, « *lorsqu'une telle dérogation est nécessaire pour concilier le droit à la protection des données à caractère personnel et la liberté d'expression et d'information* ».

Ainsi, le responsable du traitement n'est pas soumis au principe de la limitation de la durée du traitement, au principe d'interdiction de traiter des données « *sensibles* » (données de santé, données relatives aux opinions politiques, données relatives aux condamnations pénales, etc.) ou encore au principe de transparence.

Par ailleurs, il n'est pas tenu de faire droit à certaines demandes d'exercice de droits des personnes concernées, tels que le droit d'accès, le droit de rectification et le droit à la limitation du traitement. Toutes les autres dispositions du RGPD et de la loi « *Informatique et libertés* » ont, en revanche, vocation à s'appliquer à de tels traitements et notamment le principe de minimisation des données visé à l'article 5.1.c du RGPD.

L'affaire[1]

Une plainte avait été déposée auprès de l'autorité espagnole de protection des données (l'AEPD), au motif que plusieurs médias avaient publié sur leur site web l'enregistrement audio de la déclaration faite devant un juge par une victime anonyme de viols. Cette diffusion visait à informer l'opinion publique sur le déroulement d'un procès dans une affaire très médiatisée. Il est précisé que la voix de la victime, racontant les détails des viols qu'elle avait subis, était clairement audible.

Après avoir rappelé que la voix d'une personne est une donnée à caractère personnel dès lors que cette personne peut-être identifiée par sa voix (« *la publication de la voix de la victime, seule et sans déformation, lui fait courir un risque certain d'être identifiée par des personnes ignorant sa qualité de victime* »), l'AEPD a estimé que la diffusion de l'enregistrement par le média en cause est un traitement soumis aux dispositions du RGPD : « *L'inclusion de la voix d'une personne dans des publications journalistiques, qui identifie*

ou rend identifiable une personne, implique le traitement de données à caractère personnel et, par conséquent, le responsable du traitement qui effectue le traitement est tenu de respecter les obligations énoncées dans le RGPD et la LOPDGDD (loi espagnole de protection des données). »

Selon l'autorité espagnole de protection des données, un tel traitement est illicite en ce qu'il méconnaît le principe de minimisation des données (article 5.1. c) du RGPD), le média ayant traité des « *données excessives* », c'est-à-dire des données qui n'étaient pas « *nécessaires* » à la finalité du traitement, traitement dont la légitimité n'est en revanche pas remis en cause : « *L'intérêt public évident des nouvelles n'est pas nié, étant donné l'intérêt général pour les affaires pénales, et, dans ce cas précis, il ne s'agit pas de faire reculer le droit fondamental à la liberté d'information en raison de la prévalence du droit fondamental à la protection des données à caractère personnel, mais plutôt de les rendre pleinement compatibles de manière que les deux soient absolument garantis* ». « *Ce n'est [donc] pas la liberté d'information des médias qui est en cause, ajoute l'AEPD, mais plutôt la mise en balance avec le droit à la protection des données personnelles spécifiques à la voix* ». En d'autres termes, une telle situation aurait pu être évitée si le média en cause avait utilisé des « *procédures techniques visant à empêcher la reconnaissance de la voix, comme la déformation de la voix de la victime ou la transcription du récit du viol, qui sont toutes les deux des mesures de sécurité appliquées par les médias en que telles, selon les cas* ».

Quelles recommandations ?

Cette affaire est une des premières dans laquelle le RGPD a été invoqué à l'encontre d'un média aux fins de contester la licéité d'une publication/diffusion. On constate que le principe de minimisation est, dans cette optique, parfaitement adapté et s'analyse comme un outil juridique efficace et complémentaire aux outils traditionnels comme l'article 9 du code civil sur le droit au respect de la vie privée.

Alexandre FIEVEE
Avocat associé
DERRIENNIC Associés

Notes

(1) AEPD, PS/00191/2022.

DOCTRINE

RGPD

Consultations abusives de données à des fins privées

Comme chaque mois, Alexandre Fievée tente d'apporter des réponses aux questions que tout le monde se pose en matière de protection des données personnelles, en s'appuyant sur les décisions rendues par les autorités nationales de contrôle au niveau européen et les juridictions européennes. Ce mois-ci, il se penche sur la problématique des traitements réalisés à des fins privées par des personnes ayant un accès légitime à une base de données dans le cadre de leurs fonctions.

Il ressort des termes de l'article 5.1a du RGPD que les données à caractère personnel doivent être traitées « *de manière licite, loyale et transparente* » au regard de la personne concernée. La licéité du traitement suppose qu'il repose sur une base légale, dont la liste exhaustive figure à l'article 6.1. Le respect de ces principes et conditions de licéité du traitement de données personnelles s'impose au responsable du traitement, défini comme « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement* ».

Lorsqu'un salarié ou un agent traite des données personnelles hors du cadre fixé par l'organisme pour lequel il travaille parce que le traitement est réalisé à des fins exclusivement privées, doit-on considérer cette personne – qui a défini elle-même les finalités du traitement - comme responsable du traitement ? Est-ce que ce traitement est par conséquent de facto illicite en application des articles 5.1 et 6.1 du RGPD ? C'est à ces questions que l'autorité belge de protection des données (APD) a eu à se prononcer.

L'affaire[1]

La plaignante avait découvert, en vérifiant l'historique des consultations de ses données au Registre national des personnes physiques, que ses données avaient été consultées le 4 septembre 2019 au moyen de l'outil de la Banque-carrefour de la sécurité sociale (BCSS). Dans le cadre de l'exercice de son droit d'accès, la plaignante a compris que cette consultation avait été faite, à des fins privées, par la fille de son ancien compagnon, assistante sociale dans un Centre provincial d'action sociale (CPAS), qui, dans le cadre de ses fonctions, avait un accès à la BCSS. C'est dans ce contexte que la plaignante a déposé une plainte auprès de l'autorité belge de protection des données sur le fondement de l'article 5.1.a du RGPD.

Après avoir rappelé que le CPAS doit être considéré comme responsable du traitement au titre des consultations des données à caractère personnel de la BCSS, l'autorité belge a précisé qu'il convient de distinguer les consultations réalisées par le personnel du CPAS dans le cadre des missions de ce dernier, des consultations « *abusives opérées à des fins privées* ». Sur cette base, l'APD a considéré que « *bien qu'ayant utilisé les moyens mis à sa disposition par [le CPAS], et dans la mesure où la défenderesse a traité les données à caractère personnel de la BCSS pour ses propres finalités, c'est-à-dire en dehors du cadre de ses tâches en tant qu'agent du [CPAS], la défenderesse doit être considérée comme un responsable du traitement pour les consultations de la BCSS, spécifiquement pour celles réalisées à des fins privées* ».

Quant à la licéité du traitement ainsi opéré, l'autorité belge de protection des données a estimé qu'en omettant de respecter la finalité de l'accès qui lui avait été attribué, la défenderesse a consulté le Registre national « *sans fondement légal adéquat* » et donc en violation de l'article 6.1 du RGPD. Ce manquement doit être, selon l'APD, combiné avec celui de l'article 5.1.a du même texte, qui impose un principe de licité, de loyauté et de transparence applicable à tout traitement. Dans ce contexte, la Chambre contentieuse a décidé d'avertir la défenderesse.

Concernant l'obligation de sécurité qui pèse sur le CPAS, l'autorité de contrôle a d'abord relevé que s'il est en mesure d'identifier l'agent ayant consulté les données personnelles du Registre national ainsi que la date de consultation, il était en revanche incapable de connaître la finalité de la consultation et la nature des données consultées. Puis l'APD a étonnamment procédé à un classement sans suite de la plainte pour « *motif technique* », celle-ci n'étant pas suffisamment étayée par des preuves de l'existence d'une atteinte au RGPD ou aux lois de protection des données personnelles.

Quelles recommandations ?

Ce type de décisions sanctionnant le traitement de donnée personnelles à des fins privées n'est pas isolé. D'autres autorités nationales de protection des données – notamment les autorités allemandes dans cadre de traitements réalisés par des policiers - ont eu l'occasion de qualifier le salarié/l'agent de responsable du traitement après avoir constaté que le traitement litigieux avait été réalisé à des fins privées.

Pourtant une telle solution ne s'impose pas. Il ne faut pas oublier que si le RGPD s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier, il ne s'applique pas au traitement effectué « *par une personne physique dans le cadre d'une activité strictement personnelle ou domestique* » (article 2 du RGPD).

Le considérant 18 du règlement oppose, à cet égard, la notion d'activité « *strictement personnelle ou domestique* » à celle qui est « *sans lien avec une activité professionnelle ou commerciale* ». Dans ces conditions, on peut légitimement se demander si une telle solution est conforme au RGPD. Peut-être que l'outil juridique le plus adapté – en droit français - serait l'article 226-21 du code pénal qui sanctionne « *le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité* ». A suivre.

Alexandre FIEVEE
Avocat associé
DERRIENNIC Associés

Notes

(1) APD, Décision 16/2023, 27 février 2023.

LE DOSSIER MEDICAL A L'EPREUVE DU DROIT

Par un arrêt du 11 avril 2023, la Cour administrative d'appel de Paris a statué sur la licéité d'un traitement de données à caractère personnel relatif au dossier médical d'un patient. Cette décision est particulièrement éclairante sur les contours des droits et obligations des parties prenantes : la personne concernée/le patient, d'une part, et le responsable du traitement/l'établissement ou le professionnel de santé, d'autre part.

L'affaire concerne une patiente qui avait été prise en charge, à deux reprises, par un psychiatre dans le service d'urgence d'hôpitaux relevant de l'AP-HP. Deux années plus tard, ladite patiente a demandé à l'AP-HP de supprimer et de modifier certaines de ses données à caractère personnel, notamment celles relevant de ses « *antécédents sociaux-familiaux* », mais aussi celles relatives à sa vie personnelle (y compris sa sexualité). Selon la patiente, ces données auraient été recueillies et ajoutées à son dossier médical sans son consentement ni information sur ses droits (en particulier son droit à rectification).

A défaut de réponse favorable, la patiente a saisi le Tribunal administratif de Paris afin d'obtenir de la part de l'AP-HP le paiement de la somme de 10.000 euros au titre du préjudice qu'elle aurait subi par suite d'un tel traitement considéré comme illicite. La juridiction de 1ère instance ayant rejeté sa requête, la patiente a interjeté appel.

Dans sa décision, la Cour administrative d'appel de Paris a considéré, d'une part, que les données en cause « *peuvent contribuer à l'appréciation de* [l']*état psychologique* [de la patiente] *et à la prise de décisions thérapeutiques* », d'autre part, qu'elles *« constituent des données qui peuvent être inscrites au dossier médical de la patiente* » et qu'enfin le consentement de la patiente au recueil de telles données n'était pas nécessaire.

La juridiction a également estimé que l'AP-HP était en droit de ne pas procéder à l'effacement de ces données, tel que sollicité par la patiente, dès lors que de telles données permettent de « *contribuer à l'appréciation de l'état de santé de* [la patiente]*et à la prise de décisions thérapeutiques* ».

Pour aboutir à une telle conclusion, les juges d'appel se sont fondés sur deux textes :

- Le Code de la santé publique et, plus particulièrement son article R. 1112-2, selon lequel « un dossier médical est constitué pour chaque patient hospitalisé dans un établissement de santé public ou privé », étant précisé que ce dossier médical peut contenir « les informations formalisées recueillies lors de l'accueil au service des urgences ou au moment de l'admission et au cours du séjour hospitalier, et notamment : (…) les motifs d'hospitalisation (…) la recherche d'antécédents et de facteurs de risques ; (…) les conclusions de l'évaluation clinique initiale ; (…) » ;

- Le RGPD, et plus précisément ses articles 6.1.e), 9.2.h) et 17.3c) qui prévoient notamment : la licéité d'un traitement de données personnelles lorsqu'il est nécessaire à l'exécution d'une mission d'intérêt public ; la possibilité de traiter des données de santé ou relatives à la sexualité aux fins de médecine préventive, de diagnostics médicaux la gestion des services de soins de santé ou encore la garantie de normes élevées de qualité et de sécurité des soins de santé ; ainsi qu'une exception au droit à l'effacement de la personne concernée pour des motifs d'intérêts publics dans le domaine de la santé publique.

En revanche, la Cour a considéré que l'AP-HP avait commis une faute en n'informant pas la patiente de son droit à rectification des données mentionnées dans son dossier médical comme l'exige l'article 13.2 du RGPD.

Aucun préjudice pour « *atteinte la vie privée* » n'a été retenu. La Cour a effectivement souligné que les professionnels de santé – ayant accès aux données litigieuses permettant « *de contribuer à une meilleure prise en charge médicale de l'intéressée* » - étaient soumis au secret professionnel sans qu'il ne soit démontré qu'un tel secret aurait été violé.

La demande de la patiente a ainsi de nouveau été rejetée.

Cette jurisprudence donne ainsi des « clés » d'appréciation relativement aux droits des patients, à l'effacement et à la modification des données personnelles portées à leur dossier médical, et à la licéité du traitement de telles données par les professionnels de santé.

Lire l'article original : ici

Source : : ici

PANORAMA EUROPÉEN

PANORAMA DE QUELQUES DECISIONS RENDUES PAR DES AUTORITÉS NATIONALES DE CONTRÔLE

Les signatures des représentants syndicaux ne doivent pas apparaître sur les documents affichés

AEPD (Espagne), 23 août 2022

L'autorité de contrôle espagnole a sanctionné un employeur pour avoir publié un procès-verbal contenant les signatures de représentants syndicaux.

Un employeur a publié le procès-verbal du comité d'entreprise sur le tableau d'affichage des communications syndicale et a transmis ledit procès-verbal sur un groupe WhatsApp.

Les représentants syndicaux, dont les signatures apparaissaient sur le procès-verbal, ont considéré que le traitement était contraire au RGPD et ont déposé une plainte auprès de l'autorité de contrôle espagnole.

Au cours de son enquête, cette dernière a considéré qu'un « *procès-verbal [qui] contient l'identification des signataires avec leur nom, prénom et position […] créé une situation de risque pour les signataires* ».

En effet, « *il ne peut être ignoré que la publication de la signature manuscrite peut générer une situation de risque en raison de la possibilité de reproduction par une personne qui accède au document* ».

Partant de ce constant, l'autorité de contrôle a recommandé la suppression de *« toutes les signatures manuscrites des documents à condition que l'absence de signature soit complétée par une mention qui montre que l'original a effectivement été signé* ».

L'autorité de contrôle, qui a ainsi considéré que l'employeur n'avait pas respecté les principes de minimisation des données (article 5.1.c du RGPD) et de confidentialité (article 5.1.f), a infligé une amende de 2000 € au responsable du traitement.

Source : ici

Quand le juge perd un clé USB, c'est le tribunal qui est sanctionné

UODO (Pologne), 19 janvier 2023

En septembre 2020, un tribunal polonais (responsable du traitement) a notifié à l'autorité de contrôle polonaise une violation de données à la suite de la perte de trois clés USB (une professionnelle cryptée et deux personnelles non cryptées) par un juge.

Ces clés contenaient, entre autres, des projets de jugements, des pièces judiciaires et plus largement de nombreuses données personnelles (y compris des données sensibles) en lien avec des justiciables. Bien que la quantité de données personnelles « *n'ait pas pu être déterminée* », les clefs comportaient « *les données relatives aux affaires judiciaires du juge depuis 2004* ».

Au cours de son enquête, l'autorité de contrôle a constaté que le tribunal avait réalisé en 2019 une analyse des risques qui concluait qu'il existait *« un risque de perte de confidentialité en raison de l'accès aux données par des personnes non autorisées du fait du stockage sur des supports amovibles privés non sécurisés* ».

A cette date, le responsable du traitement avait envisagé une solution technique de réduction des risques consistant à *« instaurer un blocage de l'utilisation des supports de stockage privés [lesdits supports n'étant plus reconnus par le système informatique] et une obligation d'utiliser uniquement des supports de stockage cryptées ».*

Considérant que le risque était modéré, le responsable du traitement n'a cependant pas mis en œuvre cette solution technique de blocage, mais a uniquement « *interdit formellement d'utiliser des supports de stockage privés* ».

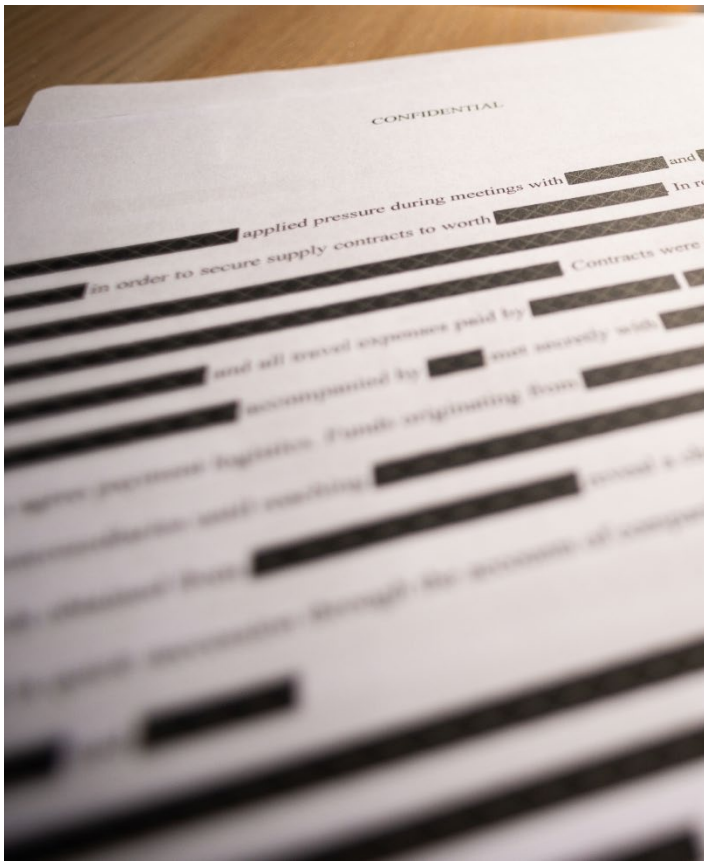
Urząd Ochrony Danych Osobowych

Jugeant cette dernière mesure insuffisante, et considérant que la solution technique de blocage aurait dû être implémentée par le responsable du traitement, l'autorité de contrôle polonaise a infligé au tribunal une amende d'environ 6700 € pour n'avoir pas pris les mesures de sécurité adaptées aux risques, en violation des articles 5 (principe de confidentialité), 24 (principe de responsabilité), 25 (privacy by default) et 32 (sécurité du traitement) du RGPD.

Source : ici

La transmission d'un jugement non anonymisé par un avocat viole le RGPD

AEPD (Espagne), 25 août 2022



L'autorité de contrôle espagnole a considéré que le transfert d'un jugement non anonymisé sans le consentement des parties était dépourvu de base légale.

Dans le cadre d'un contentieux devant les juridictions espagnoles, une avocate, (visiblement satisfaite du jugement obtenu en faveur de sa cliente), avait transmis ledit jugement non anonymisé à d'autres personnes sur WhatsApp « *dans le but de se promouvoir professionnellement* ».

Apprenant l'existence dudit transfert, sa cliente déposa une plainte devant l'autorité de contrôle espagnole.

Au cours de son enquête, cette dernière a considéré qu'en diffusant un jugement sans le consentement de sa cliente, l'avocate (i) avait traité des données personnelles sans base légale, en violation de l'article 6 du RGPD et, de manière plus étonnante, (ii) avait manqué aux principes d'intégrité et de confidentialité, en violation de l'article 5 §1 f du RGPD.

Compte tenu de ce qui précède, l'autorité de contrôle espagnole a infligé une amende de 4000 euros à l'avocate.

Source : ici

Dossier médical : obligation de conservation et de transmission en cas de demande d'exercice des droits

NAIH (Hongrie), 9 juin 2022

L'autorité de contrôle hongroise a sanctionné un médecin pour (i) n'avoir pas indiqué l'adresse permettant aux personnes concernées d'exercer leurs droits et (ii) n'avoir pas gardé le dossier médical d'une patiente.

Une femme s'était rendue à l'hôpital et avait découvert que son enfant était mort *in utero* depuis plusieurs jours, alors qu'elle venait d'effectuer une visite chez son gynécologue-obstétricien, qui n'avait rien décelé.

La femme a alors pris contact avec son gynécologue. Ce dernier ne répondant pas, elle a transmis directement, puis par l'intermédiaire de son conseil, deux courriers recommandés à l'adresse du cabinet médical afin d'exercer son droit d'accès et d'obtenir une copie de l'intégralité de son dossier médical pendant toute la phase de grossesse.

Les courriers n'ayant pas été délivrés et les demandes étant restées sans réponse, la femme a déposé une plainte auprès de l'autorité de contrôle Hongroise.

Au cours de l'enquête, le médecin a indiqué à l'autorité de contrôle n'avoir jamais reçu les courriers recommandés et ne pas être informé de la demande puisqu'il n'a pas d'adresse postale audit cabinet. Plus précisément, il a indiqué utiliser les locaux « *sur la base d'un accord oral* », quelques heures par jour et sans possibilité d'y recevoir de courrier.

Constatant (i) que les courriers de la femme étaient envoyés à la même adresse que l'endroit où elle avait effectué ses consultations médicales et (ii) que les mentions d'informations ne précisaient pas l'endroit où les demandes d'exercice des droits devaient être effectuées, l'autorité de contrôle a considéré que le gynécologue n'avait pas respecté son devoir de faciliter l'exercice des droits des personnes, en violation des articles 12 et 13 du RGPD.

Nemzeti Adatvédelmi és Információszabadság Hatóság

Selon l'autorité de contrôle, « *si la personne concernée ne reçoit pas d'informations explicites sur l'adresse à laquelle la demande doit être faite, il est raisonnable pour elle d'envoyer la demande à l'adresse du cabinet médical où elle se rend régulièrement* ».

L'autorité a également constaté que le médecin n'avait pas conservé le dossier médical de la patiente, et plus largement ne conservait presque *« aucune documentation médicale »,* et ce en violation de la réglementation hongroise.

Face à l'absence de dossier médical, l'autorité n'a pas pu (i) enjoindre au gynécologue de transmettre ledit dossier, ni (ii) considérer que le gynécologue avait violé le droit du requérant d'obtenir une copie de son dossier médical.

En revanche, l'autorité de contrôle a considéré que le gynécologue avait manqué à son obligation de transparence et que « *l'absence de documentation des processus ayant conduit à la tragédie, [avait] empêché la requérante d'exercer ses droits et d'obtenir l'accès à ses données de santé* ».

Compte tenu de tout ce qui ce qui précède, l'autorité de contrôle hongroise a considéré que le médecin avait violé les articles 5.1.a (principe de transparence), 12 (manquement l'obligation de faciliter l'exercice des droits) et 13 (absence d'information sur les coordonnées du responsable du traitement) du RGPD. Le médecin s'est vu infligé une amende d'environ 1600 €.

Source : ici

ACTUALITÉS DU CABINET

DERRIENNIC ASSOCIÉS PROPOSE UN PROGRAMME DE FORMATION DE 35 HEURES POUR LA PRÉPARATION À LA CERTIFICATION DPO

OBJECTIFS

1/ Acquérir les compétences, les connaissances et le savoir-faire attendus par la CNIL et permettre au collaborateur de se présenter à l'examen de certification en maximisant ses chances de succès.

2/ Indépendamment de la certification, la formation permet à l'apprenant de se familiariser avec la matière et d'acquérir les compétences, les connaissances et le savoir-faire pour :

- analyser une situation impliquant un traitement de données personnelles ;
- définir et appréhender les problématiques, les enjeux et les risques qui en découlent ;
- prendre les décisions qui s'imposent en concertation avec l'équipe « DPO ».

CONTENU DE LA FORMATION

Partie 1 - Réglementation générale en matière de protection des données et mesures prises pour la mise en conformité
Partie 2 - Responsabilité (Application du principe d'« Accountability »)
Partie 3 - Mesures techniques et organisationnelles pour la sécurité des données au regard des risques

COÛT

3000€ HT/personne

INTERVENANT

Alexandre FIEVEE
Avocat Associé
01.47.03.14.94
afievee@derriennic.com

CLASSEMENTS
Alexandre Fievee figure dans le classement BestLawyers dans la catégorie « *Information Technology Law* » (2023).
Il a également fait en 2020 son entrée dans le classement Legal 500 dans la catégorie *« Next Generation Partners* ».

RENSEIGNEMENTS PRATIQUES

Prochaine session en 2023 :
Sur demande.
Lieu de la formation :
Au cabinet Derriennic Associés (5 avenue de l'opéra - 75001 Paris) ou en visio-conférence.
Inscription et informations :
afievee@derriennic.com