NEWSLETTER RGPD/DATA

NUMÉRO 62 ● 2024

SOMMAIRE

ACTUALITE

VU DANS LA PRESSE

ACTUALITES DU CABINET

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

ACTUALITE

UN EMPLOYEUR PEUT-IL PRODUIRE EN JUSTICE DES COURRIELS REÇUS POSTERIEUREMENT AU DEPART D'UN SALARIE ?

La Cour d'appel de Douai a eu à apprécier, dans un arrêt du 28 mars 2024, la recevabilité et la licéité de courriers électroniques reçus par des salariés, postérieurement à leur départ de l'entreprise, et produits par leur ancien employeur à titre de preuve.

Des courriels reçus sur la messagerie électronique des salariés, après leur départ

Trois salariés d'une société, spécialisée dans la formation de négociateurs, ont démissionné de façon concomitante et ont fait immatriculer plusieurs sociétés ayant des objets sociaux proches de celui de leur précédent employeur.

Ce dernier, estimant que ses anciens salariés se livraient à des actes de concurrence déloyale, de parasitisme et de dénigrement, a été autorisé, par ordonnance sur requête du président du Tribunal de commerce, à réaliser des investigations et saisies aux sièges des sociétés nouvellement créées.

Afin d'obtenir cette ordonnance, l'ex-employeur a produit en justice des courriels reçus par ses anciens salariés, postérieurement à leur départ.

Prétextant l'absence de tout motif légitime fondant ces mesures, les sociétés ayant fait l'objet des saisies ont sollicité la rétractation de l'ordonnance « 145 », qu'ils ont obtenue. L'ancien employeur a interjeté appel de la décision de rétractation.

Des courriels « interceptés » en violation des recommandations CNIL

Devant la Cour d'appel, les intimées ont demandé que les courriels interceptés sur les anciennes adresses professionnelles et messageries des trois salariés soient écartés des débats.

En effet, pour les intimées, la production de ces pièces en justice :

- Est dépourvue de base légale, d'une part, et
- Ne respecte pas les recommandations de la CNIL, selon lesquelles l'employeur se doit de « *supprimer l'adresse nominative de l'employé une fois qu'il a quitté l'entreprise et d'avertir l'employé de la date de fermeture pour lui permettre de transférer ses messages privés vers sa messagerie personnelle* », d'autre part. En effet, certains courriels produits par l'appelante avaient été adressés par d'anciens clients de la société, postérieurement aux départs des salariés. Cela indique donc que les adresses électroniques étaient toujours actives après le départ des salariés.

Des courriels non seulement recevables, mais également « licites »

La Cour d'appel rappelle que :

- Les messages adressés ou reçus sur une messagerie électronique sont des données à caractère personnel ;

- Ne respecte pas les recommandations de la CNIL, selon lesquelles l'employeur se doit de « *supprimer l'adresse nominative de l'employé une fois qu'il a quitté l'entreprise et d'avertir l'employé de la date de fermeture pour lui permettre de transférer ses messages privés vers sa messagerie personnelle* », d'autre part. En effet, certains courriels produits par l'appelante avaient été adressés par d'anciens clients de la société, postérieurement aux départs des salariés. Cela indique donc que les adresses électroniques étaient toujours actives après le départ des salariés.

Des courriels non seulement recevables, mais également « licites »

La Cour d'appel rappelle que :

- Les messages adressés ou reçus sur une messagerie électronique sont des données à caractère personnel ;
- « *Les courriels adressés et reçus par le salarié à l'aide de l'outil informatique mis à sa disposition par l'employeur pour les besoins de son travail sont présumés avoir un caractère professionnel, en sorte que l'employeur est en droit de les ouvrir hors la présence de l'intéressé et les consulter, sauf si le salarié les identifie comme personnels* ».

Il en résulte que, pour la Cour, « *bien que plus de six mois après leur départ de l'entreprise, les [appelantes] n'aient pas procédé à la fermeture de ces boîtes, comme le recommande la CNIL notamment dans son avis produit aux débats, il ne peut lui être reproché la consultation de courriels qui n'avaient pas été estampillés 'personnels' et qui émanaient de clients du groupe dont il n'était pas démontré qu'ils avaient eu connaissance du départ des salariés de l'entreprise*. »

La Cour d'appel en déduit que les appelantes avaient bien un intérêt légitime à connaitre des courriels en cause.

Ainsi, pour la Cour d'appel, les courriels produits par l'employeur étaient non seulement recevables, mais également licites, nonobstant les requêtes formulées par les salariés tendant à la fermeture de leurs messageries respectives : « *Le fait que [les anciens salariés] aient sollicité (…) la fermeture de leurs boites de messagerie professionnelles ne retire pas à ces éléments de preuve un caractère licite et ne justifie pas d'exclure ces deux pièces des débats* ».

Source : ici

DES INFORMATIONS – A L'EVIDENCE – NON IDENTIFIANTES QUALIFIEES DE DONNEES PERSONNELLES

Des informations, même indirectement identifiantes, peuvent être qualifiées de données à caractère personnel, selon le RGPD. Mais comment déterminer qu'une information identifie indirectement une personne physique ? Quels sont les critères à prendre en compte ? La Cour de Justice de l'Union Européenne a récemment apporté des nouveaux éclairages sur cette question.

Le litige : des informations non directement identifiantes figurant dans un article de presse

L'affaire concernait l'Office européen de lutte anti-fraude (OLAF), lequel a publié un communiqué de presse comportant notamment les informations suivantes : *« une fraude complexe impliquant une scientifique grecque et son réseau de chercheurs internationaux a été découverte par les enquêteurs* » ; « *l'affaire porte sur une subvention d'un montant d'environ 1,1 million d'euros accordée par l'[ERCEA] à une université grecque. Ces fonds étaient destinés au financement d'un projet de recherche mené sous la responsabilité d'une jeune scientifique prometteuse, dont le père travaillait dans l'université en question. Le projet comportait un réseau de plus de 40 chercheurs du monde entier placé sous la direction de la scientifique grecque.* ».

Un journaliste d'investigation allemand avait, par la suite, publié, sur le réseau social Twitter, un article en lien avec ce communiqué, dans lequel il identifiait la scientifique concernée en indiquant son nom et son prénom.

A l'occasion d'un litige opposant l'OLAF et la scientifique, la CJUE a été amenée à se prononcer sur la caractérisation des informations figurant dans le communiqué de presse en tant que données à caractère personnel.

La position de la CJUE : des informations non directement identifiantes peuvent être qualifiées de données à caractère personnel, notamment par combinaison avec des informations provenant d'autres sources

Dans sa décision, la CJUE a rappelé et précisé sa jurisprudence relativement à la notion d'identification indirecte d'une personne physique.

Pour la CJUE, il est « *inhérent à la notion d'identification indirecte* » d'une personne physique que des informations supplémentaires doivent être combinées avec les données en cause aux fins de l'identification de la personne concernée.

Aussi, la CJUE a indiqué que « *le fait que ces informations supplémentaires relèvent d'une autre personne ou source que celle du responsable du traitement des données en cause n'exclut aucunement (…) le caractère identifiable d'une personne* ». Pour autant, selon la CJUE, *« la circonstance qu'un journaliste d'investigation a, comme en l'occurrence, diffusé l'identité d'une personne visée par un communiqué de presse ne saurait permettre, à elle seule, de conclure que les informations figurant dans ce communiqué doivent nécessairement être qualifiées de données à caractère personnel* ».

Par ailleurs, la CJUE a jugé que le droit de l'UE *« ne pose aucune condition quant aux individus susceptibles d'identifier la personne à laquelle une information est liée* ».

En l'espèce, la Cour a relevé que le communiqué de presse litigieux contenait des informations relatives au genre de la personne concernée, à sa nationalité, à l'activité de son père, au montant de la subvention du projet scientifique et à la localisation géographique de l'entité accueillant le projet scientifique. Ces données prises ensemble « *comportent des informations de nature à permettre l'identification de la personne visée dans le communiqué notamment par des personnes travaillant dans le même domaine scientifique et connaissant son parcours professionnel* ».

Aussi, selon la Cour, « *un communiqué de presse visant des comportements prétendument illégaux, tels que des actes de fraude ou de corruption, est susceptible de susciter un intérêt certain auprès du public et d'amener ses lecteurs, notamment des journalistes, à effectuer des recherches sur la personne visée par le communiqué ».* Or, la Cour a relevé que l'ERCEA, organisme ayant octroyé la subvention, décrit sur son site internet les 70 projets qu'elle finance, et que les publications comportent des *« éléments clés permettant à l'internaute de trouver les informations souhaitées, comme le nom du responsable du projet, le nom de l'institution d'accueil ou encore le montant du financement* ».

« *Dans un tel contexte, l'effort consistant à procéder à de telles recherches sur un site Internet, en parcourant la description de quelques 70 projets financés figurant sur ce site, combinées avec d'autres recherches sur Internet permettant vraisemblablement d'obtenir le nom et d'autres identifiants de la personne visée par le communiqué de presse litigieux, n'apparaît aucunement démesuré, de sorte que le risque d'identification de la requérante par les journalistes ou d'autres personnes ne connaissant pas son parcours professionnel* » n'est pas « insignifiant », a estimé la CJUE.

Les informations contenues dans le communiqué de presse litigieux relèvent ainsi, selon la Cour, de la notion de « *données à caractère personnel* ».

Cette jurisprudence illustre, à nouveau, le caractère particulièrement large de la notion de données à caractère personnel. En effet, celle-ci peut s'appliquer à des informations qui ne semblent pas, à l'évidence, identifiantes, mais qui peuvent être considérées comme telles par la combinaison et l'analyse d'autres informations (i) quand bien même ces autres informations figurent dans d'autres sources que la source des informations premières, et (ii) en tenant compte du risque d'identification par le public susceptible d'être intéressé par lesdites informations.

Source : ici

LES PRIORITES DU CEPD POUR 2024-2027

Dans un document publié le 18 avril 2024, le CEPD a défini ses priorités pour la période 2024-2027 et a clarifié la mise en œuvre des mécanismes de recours de la décision d'adéquation concernant les Etats-Unis (« Data Privacy Framework », « DPF »).

Dans un document sobrement intitulé « EDPB Strategy 2024-2027 », le CEPD a indiqué que ses priorités pour la période 2024-2027 s'articuleront autour de 4 piliers, détaillés ci-après.

La publication de ce document s'est accompagnée d'une documentation visant à clarifier le mécanisme de recours du DPF.

Pillier 1 – Renforcer l'harmonisation et promouvoir la conformité

Le CEPD continuera à fournir des lignes directrices sur des sujets d'importance, à développer des outils destinés à une audience plus large et à produire du contenu accessible à des « non-experts », notamment des enfants et des PME.

Pillier 2 – Renforcer une culture commune de l'application et une coopération efficace

Le CEPD continuera à identifier des dossiers stratégiques, pour lesquels la coopération sera priorisée et l'enquête suivra une approche harmonisée. Le CEPD renouvellera son engagement en faveur d'un fonctionnement souple du mécanisme d'autorité chef de file.

Pillier 3 – Sauvegarder la protection des données dans le paysage numérique et inter réglementaire et développement

Le CEPD fournira des lignes directrices quant aux interactions entre le RGPD et les autres normes européens, telles que l'IA Act. Le CEPD continuera à surveiller et évaluer les nouvelles technologies numériques et à promouvoir une approchée centrée sur l'humain, notamment l'IA et l'identité numérique.

Pillier 4 – Contribuer au dialogue mondial sur la protection des données

Le CEPD aidera l'échange d'informations et de coopérations entre autorités de contrôles dans le cadre de forums internationaux, facilitera et renforcera la coopération entre les autorités de contrôle européennes et non-européennes.

Clarifications quant au mécanisme de recours du Data Privacy Framework

Enfin, le CEPD a annoncé avoir adopté des documents relatifs au mécanisme de recours du DPF, visant à faciliter sa mise en œuvre :

- Un règlement intérieur ;
- Une note d'information publique ;
- Des formulaires de plainte types.

Pour l'heure, ces documents ne semblent pas avoir été publiés par le CEPD.

Source : ici

LA CNIL RAPPELLE L'OBLIGATION D'ADAPTER LES DUREES DE CONSERVATION EN TENANT COMPTE DE LA NATURE DES DONNEES PERSONNELLES

Dans une décision du 31 janvier 2024, la CNIL a infligé une amende de 100 000 euros à PAP, la société éditrice du site internet de publication et de consultation d'annonces immobilières en ligne « De Particulier à Particulier *», notamment car celle-ci conservait les données personnelles de ses clients pour une durée excessive.*

Lors de deux contrôles diligentés en 2022, la CNIL a relevé quatre violations par la société PAP des règles imposées par le RGPD. Parmi ces violations : le manquement à l'obligation de limiter les durées de conservation des données des comptes utilisateurs. Retour sur cette décision.

La conservation pendant une durée excessive des données personnelles des clients non-facturés

La société avait indiqué qu'elle conservait les données personnelles des utilisateurs ayant recours aux services gratuits du site pendant « cinq ans à compter de la dernière connexion au *compte* », « *à des fins contentieuses et de lutte contre la fraude* », ce que la CNIL a considéré comme une durée justifiée.

Or, les agents de contrôle ont relevé qu'en réalité, les données étaient conservées pendant plus de cinq ans – cette durée allant parfois jusqu'à « *plus de dix ans* » – « *en base active, sans qu'intervienne d'archivage intermédiaire* ».

Cela constitue une violation du paragraphe (e) l'article 5-1 du RGPD[2], mais également des principes généraux de loyauté et de transparence des traitements édictés par le paragraphe (a) du même texte. Le manquement étant caractérisé, la société a dû se mettre en conformité en supprimant les « *données relatives [aux] comptes inactifs depuis plus de cinq ans* ».

La conservation pendant une durée excessive des données personnelles des clients facturés

La société conservait le contenu des annonces, le nom et le prénom, le numéro de téléphone et l'adresse électronique des clients pendant une durée de « *dix ans à compter de la date d'acceptation de la commande* », en se prévalant des dispositions du Code de la consommation.

La CNIL relève que la société proposait deux formules payantes à ses clients : soit un contrat d'une durée déterminée de trois mois pour 135€, soit un contrat sans engagement pour 59€ par mois à durée indéterminée. Pour les seconds, la société estimant ne pas être en mesure de déterminer à l'avance la durée du contrat, elle avait fait le choix de « *conserver toutes les données relatives à ces contrats pour une durée de dix ans, quel qu'en soit le montant final* ». Selon le Code de la consommation, les professionnels doivent conserver les données personnelles des consommateurs pour les contrats d'une valeur supérieure à 120€ pendant dix ans. Cependant, la CNIL précise que cette obligation ne s'applique pas aux contrats de faible valeur, c'est-à-dire inférieurs à 120€.

Ainsi, la CNIL considère que la conservation pour une durée de dix ans est pleinement justifiée pour les contrats de trois mois d'un montant de 135€ proposés par la société. En revanche, en conservant par défaut les données relatives aux « *contrat sans engagement d'un montant de 59€ par mois* », la CNIL considère que la société a violé l'article 5.1(e) du RGPD.

La CNIL souligne que « *pour assurer la sécurité des données, il est nécessaire qu'un tri soit effectué parmi ces données* » et que celles-ci *« doivent être supprimées ou faire l'objet d'un archivage intermédiaire consistant notamment en une séparation physique ou logique* ». Cette décision rappelle aux responsables de traitement l'importance de trier les données pour appliquer les mesures de purge adaptées. La CNIL encourage les DPO et les équipes opérationnelles des sites de e-commerce à collaborer pour définir les règles d'archivage et de purge en fonction de la valeur des paniers moyens.

Source : ici

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

LA TEMPERATURE CORPORELLE EST UNE DONNEE DE SANTE QUI DOIT ETRE PROTEGEE COMME UNE AUTRE

AEPD (Espagne), 8 février 2024

L'autorité de contrôle espagnole a infligé une amende à une clinique qui, pendant la crise du Covid, obligeait les patients à mesurer leur température corporelle au vu et au su de tous.

Pendant la crise du covid, les patients se présentant à la réception d'une clinique étaient sommés, conformément à la législation locale, de prendre leur température à l'aide d'un thermomètre fixé au mur situé entre la salle d'attente et la réception.

Un patient, constatant que le thermomètre affichait la mesure de la température sur un écran visible par les autres personnes présentes dans la salle d'attente, a refusé de prendre sa température. N'ayant pas été autorisé à réaliser sa prise de sang, il a déposé une plainte devant l'autorité de contrôle espagnole.

Pour sa défense, la clinique indiquait :

- Que la température d'une personne n'est pas une donnée personnelle ;
- Qu'en tout état de cause, la clinique n'est pas responsable du traitement car les relevés de température étaient effectués par les patients eux-mêmes ;
- Qu'il n'est pas démontré que, le jour où le patient s'est présenté, il y avait effectivement d'autres personnes dans la salle d'attente qui auraient pu voir sa température ;
- Que, compte tenu de l'emplacement du thermomètre et d'un dispositif d'obstruction visuelle, il était presque impossible que la température soit visible par d'autres personnes ;
- Qu'en ce qui concerne le cas d'espèce, le patient n'a pas pris sa température, et donc qu'en tout état de cause aucun traitement de ses données à caractère personnel n'a été effectué.

L'autorité de contrôle a considéré, au contraire :

- Que la température corporelle est une donnée de santé et qu'ainsi les contrôles de température peuvent constituer un traitement au sens du RGPD ;
- Que ce traitement, réalisé pendant la crise du Covid, était autorisé par la législation locale et donc reposait sur une base légale valable ;
- Que le résultat de la mesure de la température s'affichait pendant plusieurs secondes sur l'écran de l'appareil, le rendant visible des autres personnes présentes dans la salle d'attente. Qu'en conséquence, cela permettait aux autres personnes de déduire l'état de santé de la personne.

Compte tenu de ce qui précède, l'autorité de contrôle a (i) considéré que la clinique n'avait pas mis en œuvre les mesures de sécurité nécessaires pour éviter que les autres personnes puissent voir la température du patient conformément aux articles 5.1.f et 32 du RGPD et a (ii), en conséquence, infligé une amende de 20 000 euros à la clinique.

Source : ici

DENONCIATION D'UN SALARIE AUTEUR D'UNE INFRACTION AU CODE DE LA ROUTE : L'EMPLOYEUR DOIT PREALABLEMENT VERIFIER L'IDENTITE

CPLD (Bulgarie), 9 février 2023

L'autorité de contrôle bulgare a infligé une amende à un employeur qui, après avoir reçu une contravention, a dénoncé à l'administration le mauvais salarié en transmettant ses données personnelles sans vérifier l'identité du conducteur.

Un chauffeur poids lourd a reçu, de la part de l'administration, une contravention pour une infraction au code de la route qu'il aurait commise avec un véhicule de la société pendant ses horaires de travail.

Comprenant que l'administration avait obtenu ses données personnelles à la suite d'une dénonciation de son employeur, il a déposé une plainte contre ce dernier auprès de l'autorité de contrôle.

Le salarié considérait que son employeur avait transmis ses données de manière illégale à l'administration puisqu'il ne conduisait pas le véhicule en question … et pour preuve, il était en congé maladie le jour de l'infraction !

L'employeur a reconnu avoir commis une *« erreur matérielle non intentionnelle* ».

L'autorité de contrôle a considéré :

D'une part, que, si l'employeur a une base légale pour transférer les données de ses salariés à des fins de dénonciation du conducteur, tel n'est pas le cas lorsque le salarié dénoncé n'est pas le conducteur concerné ;

D'autre part, que l'employeur aurait dû procéder à une vérification du conducteur avant de fournir les données à l'administration.

Compte tenu de ce qui précède, l'autorité de contrôle a infligé une amende d'environ 5100 euros à l'employeur pour défaut de base légale.

Република България
Комисия за защита на личните данни

Source : ici

L'ENVOI D'UN COURRIEL, A UNE LISTE DE DESTINATAIRES ATTEINTS DU VIH, SANS UTILISER LA FONCTION COPIE CACHEE EST CONTRAIRE AU RGPD

ICO (Royaume-Uni), 6 mars 2024

L'autorité de contrôle anglaise a infligé une amende à un organisme éducatif qui, en transmettant un courriel aux membres d'un programme d'accompagnement des personnes atteintes du VIH sans utiliser la fonction copie cachée, a dévoilé des informations sur l'infection des destinataires.

Le 6 octobre 2022, un organisme caritatif d'éducation a transmis à 270 destinataires un courrier électronique les invitant à une conférence sur la nutrition.

L'invitation s'inscrivait dans le cadre du programme de santé positive, un programme destiné aux personnes atteintes du VIH.

Problème : le courriel a été envoyé, par erreur, en utilisant la fonction « copie » et non la fonction « copie cachée ». En conséquence, des informations relatives à l'état de santé des 270 destinataires ont été transmises.

Saisie de plusieurs plaintes, l'autorité de contrôle anglaise a considéré, outre que les données traitées par l'organisme caritatif sont des données de santé, que le responsable du traitement avait enfreint les principes de sécurité posé aux articles 5.1.f et 32 du RGPD du Royaume-Uni.

Compte tenu de ce qui précède, l'autorité de contrôle a infligé une amende de 7500 livres à l'encontre de l'organisme pour manquement aux obligations de sécurité qui pèsent sur les responsables du traitement.

Source : ici

UNE CRECHE SANCTIONNEE POUR AVOIR JETE DES DOCUMENTS A LA POUBELLE

HmbBfDI (Allemagne, Hambourg), Rapport d'activité 2023

L'autorité de contrôle allemande a sanctionné une crèche pour avoir jeté, dans des poubelles accessibles au public, des dossiers comportant des données à caractère personnel des parents et des enfants.

Un citoyen a découvert, dans les poubelles de recyclage de la commune, plusieurs dossiers jetés par une crèche.

Alertée par le citoyen, la crèche s'est contentée de demander à ce dernier de détruire les documents ou de les lui rapporter.

Saisie d'une plainte du citoyen, l'autorité de contrôle hambourgeoise a constaté que les documents jetés, accessibles au public et intacts, comprenaient de nombreuses données personnelles telles que les coordonnées bancaires, des copies de documents d'identité, mais également des certificats de vaccination et des résultats d'examens médicaux d'enfants.

Rappelant que « *l'élimination inappropriée de documents est contraire à l'article 32 du RGPD* », d'autant que les données traitées en l'espèce étaient des données sensibles, des données hautement personnelles et/ou des données concernant des personnes vulnérables, l'autorité de contrôle a infligé à la crèche une amende à de plusieurs milliers d'euros pour violation du principe de sécurité.

Source : ici

DOCTRINE

RGPD

IA et anonymisation : la commune avait tout faux

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 différentes autorités nationales de contrôle au niveau européen et les juridictions européennes. Ce mois-ci, il se penche sur la question de l'anonymisation, par une municipalité, des données personnelles d'individus avant leur analyse par une solution d'Intelligence Artificielle (IA).

Un traitement de données personnelles est soumis aux exigences du règlement européen sur la protection des données (dit « *RGPD* »). Il en résulte pour le responsable du traitement – celui qui détermine les finalités et les moyens dudit traitement – un certain nombre d'obligations, dont le respect des principes suivants : licéité, loyauté et transparence ; limitation des finalités ; minimisation ; exactitude ; limitation de la conservation et sécurité (article 5 du RGPD). En revanche, si les données sont anonymisées, le RGPD ne s'applique pas.

Que faut-il entendre par « *anonymisation* » ? La Cnil la définit comme « *un traitement qui consiste à utiliser un ensemble de techniques de manière à rendre impossible, en pratique, toute identification de la personne par quelque moyen que ce soit et de manière irréversible* »[1].

L'anonymisation ne doit donc pas être confondue avec la « *pseudonymisation* », qui est un traitement de données personnelles réalisé de telle manière qu'on ne puisse plus attribuer les données relatives à une personne physique sans information supplémentaire. En d'autres termes, « *la pseudonymisation consiste à remplacer les données directement identifiantes (nom, prénom, etc.) d'un jeu de données par des données indirectement identifiantes (alias, numéro séquentiel, etc.)* »[2]. Si la première est irréversible, la seconde ne l'est pas. Par conséquent, le traitement de données pseudonymisées reste soumis au RGPD (contrairement au traitement de données anonymisées, comme indiqué supra).

La difficulté, en matière d'anonymisation, consiste à éliminer toute possibilité de réidentification des personnes dont les données font l'objet du traitement. Afin de s'assurer que les techniques d'anonymisation utilisées ont été effectives, il convient d'appliquer les trois critères suivants : l'individualisation (il est impossible d'isoler une personne dans un jeu de données)[3] ; la corrélation (il est impossible de relier entre eux des ensembles de données distincts concernant une même personne[4] ; l'inférence (il est impossible de déduire, de façon quasi certaine, de nouvelles informations sur une personne)[5]. L'expérience montre qu'il est très compliqué de garantir une anonymisation parfaite des données. L'affaire ci-dessous en est l'illustration.

L'affaire[6]

L'histoire se passe en Italie, dans la commune de Trente. Avec le soutien d'une fondation, la municipalité avait lancé deux projets – « *Marvel* » et « *Protector* » - reposant sur une solution d'intelligence artificielle. Le premier impliquait la collecte d'informations (images et sons) dans les lieux publics au moyen de microphones et de caméra de vidéosurveillance. Selon la commune, responsable du traitement, les données étaient immédiatement anonymisées après leur collecte pour être ensuite analysées dans l'optique de détecter, au moyen d'une solution d'IA, des évènements pertinents pour la protection de la sécurité publique (rassemblements, agressions, etc.).
Le second projet comprenait notamment la collecte de messages haineux

postés sur la plateforme Twitter (« *X* ») et de commentaires postés sur YouTube afin, après analyse par une solution d'IA, de détecter d'éventuelles émotions négatives sur la religion (agressivité, colère, etc.) et donc d'identifier les risques et menaces pour la sécurité des lieux de culte.

L'autorité italienne de protection des données a été saisie de ces deux dossiers, qui, selon la municipalité, étaient conformes au RGPD. En tout état de cause, elle estimait que leur impact sur les droits et libertés fondamentaux des personnes était minime, puisque, même si des données personnelles étaient collectées, celles-ci étaient, avant leur analyse, immédiatement anonymisées. L'autorité de contrôle a eu une vision quelque peu différente de la situation, considérant que les techniques utilisées ne permettaient pas une anonymisation effective des données.

S'agissant des données audio, elle a estimé que « *la simple substitution de la voix du locuteur n'est en aucun cas adaptée à l'anonymisation des données à caractère personnel relatives à une conversation, étant donné qu'il est possible de deviner du contenu de la conversation des informations relatives au locuteur ainsi qu'à des tiers et que ces informations peuvent rendre identifiables le locuteur, ses interlocuteurs ou les tiers auxquels il est fait référence dans la conversation* ». S'agissant des images, l'autorité de contrôle a considéré comme insuffisante la technique du floutage des visages, les personnes concernées pouvant être identifiées par notamment « *d'autres caractéristiques ou éléments contextuels (tels que la corpulence, l'habillement, la position dans la scène filmée, des caractéristiques physiques particulières, etc.)* ». Quant aux auteurs des messages et commentaires publiés sur les réseaux X et YouTube, ces derniers étaient simplement pseudonymisés, puisque la municipalité s'était contentée de remplacer leur nom par un numéro ID.

L'autorité italienne de protection des données a donc considéré que les deux projets impliquaient des traitements de données personnelles et que, par conséquent, ces traitements auraient dû, « *tout au long de leur cycle vie* », être conformes au RGPD, ce qui n'était pas le cas en l'espèce, faute notamment d'avoir respecté les principes du RGPD. Le montant de l'amende a été fixé à 50 000 euros.

Quelles recommandations ?

L'IA – « *tout outil utilisé par une machine afin de reproduire des comportements liés aux humains, tels que le raisonnement, la planification et la créativité* » - est (et sera) de plus en plus présente dans nos vies, avec le développement de nouveaux produits ou services. Elle repose sur des algorithmes extrêmement consommateurs de données et son usage nécessite donc le respect de certaines précautions. De deux choses l'une : soit les données utilisées par ces algorithmes sont personnelles et, dans ce cas, il est vivement recommandé d'appliquer les principes du RGPD et de la loi « *Informatique et Libertés* » (qui peut prévoir des exigences particulières, notamment s'agissant des données de santé) ; soit les données utilisées par ces algorithmes ont été anonymisées et, dans ce cas, il convient de s'assurer que les techniques utilisées permettent de rendre impossible toute identification des personnes concernées par quelque moyen que ce soit et ce, de manière irréversible.

Alexandre FIEVEE
Avocat associé
Derriennic Associes

Notes

(1) https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles

(2) https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles

(3) Exemple donné par la Cnil : « Une base de données de CV où seuls les nom et prénoms d'une personne auront été remplacés par un numéro (qui ne correspond qu'à elle) permet d'individualiser cette personne. Dans ce cas, cette base de données est considérée comme pseudonymisée et non comme anonymisée. »

(4) Exemple donné par la Cnil : « Une base de données cartographique renseignant les adresses de domiciles de particuliers ne peut être considérée comme anonyme si d'autres bases de données, existantes par ailleurs, contiennent ces mêmes adresses avec d'autres données permettant d'identifier les individus. »

(5) Exemple donné par la Cnil : « Si un jeu de données supposément anonyme contient des informations sur le montant des impôts de personnes ayant répondu à un questionnaire, que tous les hommes ayant entre 20 et 25 ans qui ont répondu sont non imposables, il sera possible de déduire, si on sait que M. X, homme âgé de 24 ans, a répondu au questionnaire, que ce dernier est non imposable. »

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

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* » (2024).
Il a également fait en 2020 son entrée dans le classement Legal 500 dans la catégorie *« Next Generation Partners* ».

RENSEIGNEMENTS PRATIQUES

Prochaine session en 2024 :
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