NEWSLETTER RGPD/DATA

NUMÉRO 65 ● 2024

ACTUALITÉS DU CABINET P. 16

FORMATION À LA PRÉPARATION À LA CERTIFICATION « DPO ».
DATE SUR DEMANDE

SOMMAIRE

LE DROIT A L'EFFACEMENT DANS LE VISEUR DU CEPD

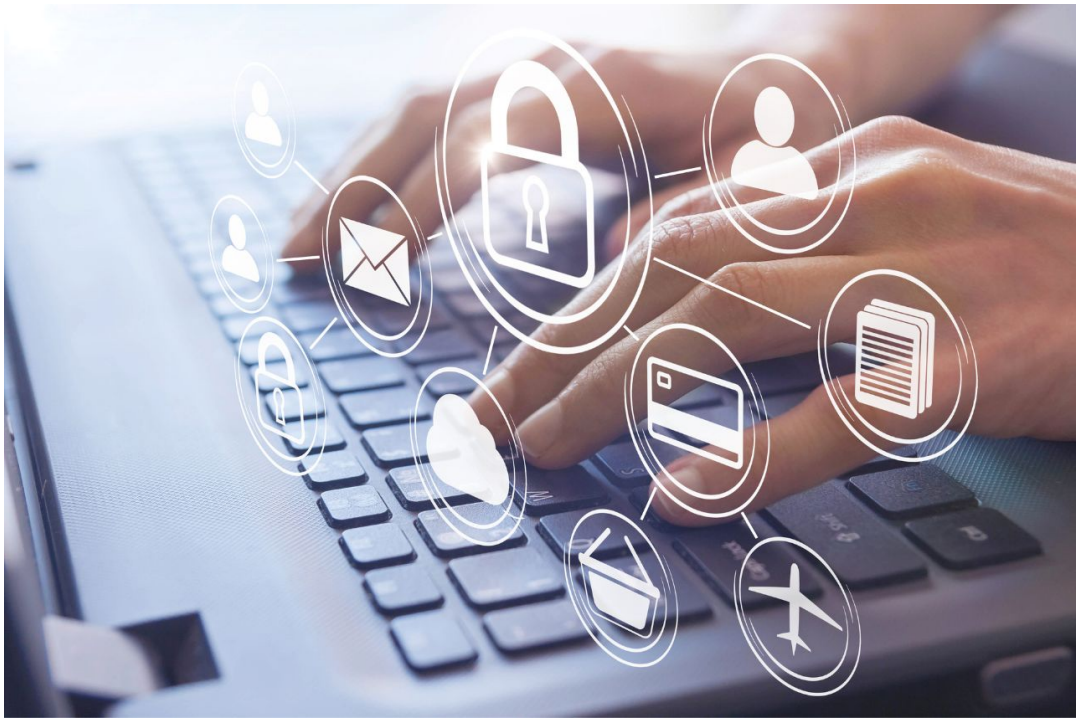
Le CEPD a annoncé que le thème de sa quatrième action coordonnée 2024 est le droit à l'effacement (article 17 du RGPD).

Dans une communication du 10 octobre 2024, le CEPD a annoncé que la prochaine action coordonnée porterait sur *« la mise en œuvre du droit à l'effacement (« droit à l'oubli ») ». « Par exemple, cela se fera en analysant et en comparant les processus mis en place par différents responsables du traitement (…) ».*

Dans l'attente de la communication de détails sur cette action coordonnée, il convient, dès à présent, de vous interroger sur l'existence d'une procédure de gestion des demandes de droit à l'effacement dans votre organisme et de sa conformité.

Une matinale sera prochainement consacrée à cette thématique…

Source : ici



VIDEOSURVEILLANCE : LE CO-PROPRIETAIRE AVAIT UN INTERET LEGITIME

L'autorité de contrôle bulgare a considéré qu'un dispositif de vidéosurveillance pouvait être fondé sur un intérêt légitime suffisant en raison de l'existence de comportements illicites antérieurs.

Un copropriétaire, possédant les 2/3 d'une habitation, avait installé, sans recueillir le consentement de l'autre copropriétaire, un dispositif de vidéosurveillance dans les parties communes.

L'autre copropriétaire, possédant 1/3 de l'habitation, a déposé une plainte auprès de l'autorité de contrôle bulgare, considérant qu'un traitement illicite de données à caractère personnel était réalisé :

- D'une part, car, en tant que copropriétaire, il n'avait pas donné son consentement à l'installation d'un tel dispositif ;

- D'autre part, car, en tant que personne concernée, il ne consentait pas à être filmé.

1/ L'installation d'un dispositif de vidéosurveillance possible sans recueil du consentement

L'autorité de contrôle a considéré que le dispositif de vidéosurveillance est soumis au RGPD car :

- D'une part, le dispositif consiste à traiter des données à caractère personnel (en l'occurrence, l'image des personnes concernées), et ;

- D'autre part, *« l'exception domestique »* ne s'applique pas en l'espèce, puisque les caméras sont situées dans des parties communes et orientées en dehors de la sphère privée.

L'autorité a, ensuite, considéré que, conformément à la réglementation locale en matière de copropriété, un copropriétaire peut installer un dispositif de vidéosurveillance sans recueillir le consentement des autres copropriétaires s'il détient plus de 50 % de la propriété, ce qui était le cas en l'espèce.

2/ L'utilisation d'un dispositif de vidéosurveillance doit reposer sur un intérêt réellement légitime

Constatant que les personnes concernées étaient dument informées à l'aide d'un panneau d'information à l'entrée du bâtiment, l'autorité de contrôle s'est toutefois demandé si le traitement mis en œuvre par le copropriétaire reposait sur une base légale valable au sens du RGPD.

L'autorité a rappelé que l'utilisation d'un dispositif de vidéosurveillance ne nécessite pas de recueillir le consentement des personnes concernées, et que le responsable du traitement peut, en principe, se fonder sur son intérêt légitime.

En l'espèce, le copropriétaire majoritaire justifiait d'un intérêt légitime car, en raison de mésententes, le copropriétaire minoritaire avait eu des comportements agressifs et avait, par ailleurs, commis de nombreux actes inciviques (ces faits étaient justifiés par le dépôt de plusieurs plaintes pénales).

Dans ce contexte, l'autorité de contrôle a considéré que l'intérêt du copropriétaire était suffisamment légitime et que cet intérêt prévalait sur le droit à la vie privée des personnes concernées.

Compte tenu de tout ce qui précède, l'autorité de contrôle a rejeté la plainte du copropriétaire minoritaire.

Source : ici

LES INSUFFISANCES D'UN DPO NE LIMITENT PAS LA RESPONSABILITE DU RESPONSABLE DU TRAITEMENT

Un employeur a été sanctionné par l'autorité de contrôle belge pour n'avoir pas correctement répondu à une demande d'exercice des droits : les insuffisances de son DPO ne sauraient limiter sa responsabilité.

Au moment de l'achat d'un produit, un consommateur avait consenti à recevoir de la prospection commerciale.

Mécontent du produit, le consommateur avait, d'une part, sollicité un remboursement partiel du prix, d'autre part, demandé la suppression de ses données personnelles et, enfin, s'était opposé à recevoir, à l'avenir, de la prospection commerciale.

Constatant qu'il recevait toujours de la prospection commerciale plusieurs mois après avoir transmis sa demande d'opposition, le consommateur a déposé une plainte auprès de l'autorité de contrôle belge.

1/ Les arguments du responsable du traitement en défense

Pour sa défense, le responsable du traitement invoquait les insuffisances de son DPO.

Plus particulièrement, il invoquait le fait que son DPO, d'une part, ne l'avait pas informé de l'ouverture d'une enquête par l'autorité de contrôle et de sa surcharge de travail, et, d'autre part, avait commis une erreur en interprétant une demande de suppression comme une demande de limitation, en n'accusant pas réception des demandes d'exercice des droits et en n'informant pas les personnes concernées une fois ces demandes traitées.

Le responsable du traitement indiquait, d'ailleurs, avoir remplacé son DPO après s'être rendu compte de ces insuffisances.

2/ Les arguments inopérants du responsable du traitement

En réponse, l'autorité de contrôle a effectivement constaté lesdites insuffisances du DPO mais a toutefois considéré :

- Que le responsable du traitement restait responsable des manquements de l'organisme au RGPD (consécutifs aux insuffisances de son DPO), notamment ceux relatifs à l'absence de réponse satisfaisante à la demande d'exercice des droits ;

- Que les arguments en défense du responsable du traitement démontraient *« que les mesures organisationnelles appropriées n'ont pas été prises pour assurer le respect du RGPD »,* et qu'en tout état de cause, le responsable du traitement aurait dû *« prendre des mesures proactives pour améliorer ses processus et assurer le respect du RGPD ».*

Compte tenu de ces constats, l'autorité de contrôle belge a infligé une amende de 172 431 € au responsable du traitement.

Source : ici

LE « SHADOWBAN » EST UNE PRISE DE DECISION AUTOMATISEE AU SENS DU RGPD

La justice hollandaise a considéré que le « shadowban » est une prise de décision automatisée au sens du RGPD et a mis en demeure X d'informer les utilisateurs, notamment, sur l'existence de ce dispositif.

Un utilisateur de l'application *« X »* (anciennement Twitter) avait posté un message (tweet) sur le réseau social critiquant le *« plan européen de lutte contre la pornographie ».*

L'utilisateur a découvert qu'il avait fait l'objet d'une restriction de type *« shadowban »*, pratique consistant à rendre invisible (ou moins visible) le compte et les messages/commentaires d'un utilisateur, sans que ce dernier en soit informé.

1/ X a eu recours à un dispositif de « shadowban »

Souhaitant connaitre l'étendue et les raisons de ce *« shadowban »,* l'utilisateur a exercé son droit d'accès auprès de X et a demandé, tout particulièrement, d'obtenir des informations (i) sur l'existence d'une prise de décision automatisée à son encontre et (ii) concernant la logique sous-jacente de la décision automatisée, ainsi que l'importance et les conséquences prévues de ce traitement.

En réponse, X n'a transmis qu'un message très général renvoyant à sa politique de confidentialité, puis, plusieurs mois plus tard, a admis que le système de détection automatique des tweets avait considéré que le tweet en question, notamment en raison de la présence du mot *« pédopornographie »*, était susceptible d'enfreindre la politique de X en matière de lutte contre la maltraitance des enfants et que, en conséquence, son tweet avait fait l'objet d'une « *restriction* » (autrement dit, d'un *« shadowban »*).

2/ Le « shadowban » est une prise de décision automatisée qui doit faire l'objet d'une information

Le tribunal de grande instance a considéré que *« la décision de restreindre le compte [de l'utilisateur] est une décision automatisée »* dès lors qu'elle *« est prise par un système qui sélectionne certains mots et décide d'imposer une restriction sur cette base »,* peu importe que *« les paramètres du système de détection aient été déterminés par des humains » tant que « la décision d'imposer une restriction n'implique pas d'intervention humaine ».*

En conséquence, le tribunal a indiqué que X aurait dû être transparent sur la prise de décision automatisée et fournir de manière proactive les informations à ce sujet, en conformité avec l'article 13 du RGPD, à savoir : (i) l'existence d'une prise de décision automatisée, (ii) les informations utiles concernant la logique sous-jacente ainsi que (iii) l'importance et les conséquences prévues de ce traitement pour la personne concernée.

Compte tenu de ce qui précède, et considérant que la première réponse de X à l'internaute n'était pas suffisante, le tribunal a mis en demeure X de répondre à la demande de droit d'accès de l'internaute en transmettant les informations ci-dessus listées, dans un délai de 1 mois et sous astreinte de 4000 € par jour de retard.

Source : ici

LE JUGE PRUD'HOMAL DOIT, LUI AUSSI, RESPECTER LE RGPD

La Cour de cassation, dans un arrêt du 3 octobre 2024, a estimé que le juge prud'homal, saisi par un salarié d'une « requête 145 » portant sur des bulletins de salaire se trouvant entre les mains de son employeur, est soumis à un certain nombre d'obligations, issues du RGPD.

Une demande de communication de bulletins de salaire

Un représentant syndical, s'estimant discriminé par son employeur en raison de son appartenance syndicale, avait engagé une action devant le conseil de prud'hommes. Sur le fondement de l'article 145 du Code de procédure civile, il demandait au juge qu'il ordonne à l'employeur la communication des historiques de carrière de neuf salariés, ainsi que de leurs bulletins de salaires. Le conseil des prud'hommes a fait droit à sa demande.

Une communication contraire au principe de minimisation

Après un appel infructueux, l'employeur a formé un pourvoi en cassation, car, selon lui, la communication des éléments demandés par le salarié constitue une violation du RGPD en ce qu'elle porte atteinte au principe de minimisation.

La Cour de cassation a, par un arrêt du 3 octobre 2024, énoncé la conduite à tenir par un juge prud'homal saisi d'une demande de communication de documents contenant des données à caractère personnel aux fins de caractérisation et de réparation de la discrimination :

« En matière prud'homal (…), il appartient au juge saisi, à l'occasion d'une action engagée devant un conseil de prud'hommes par un salarié alléguant des faits de discrimination, d'une demande de communication de documents contenant des données à caractère personnel aux fins de caractérisation et de réparation de la discrimination :

- d'abord, de rechercher si cette communication n'est pas nécessaire à l'exercice du droit à la preuve de la discrimination alléguée et proportionnée au but poursuivi (…), ensuite, si les éléments dont la communication est demandée sont de nature à porter atteinte à la vie personnelle d'autres salariés, de vérifier quelles mesures sont indispensables à l'exercice du droit à la preuve et proportionnées au but poursuivi, au besoin en cantonnant le périmètre de la production de pièces sollicitée ;

- de cantonner, au besoin d'office, le périmètre de la production de pièces sollicitées au regard notamment des faits invoqués au soutien de la demande en cause et de la nature des pièces sollicitées ;

- de veiller au principe de minimisation des données à caractère personnel, en ordonnant, au besoin d'office, l'occultation, sur les documents à communiquer par l'employeur au salarié demandeur, de toutes les données à caractère personnel des salariés de comparaison non indispensables à l'exercice du droit à la preuve et proportionnées au but poursuivi ; pour ce faire, il lui incombe de s'assurer que les mentions, qu'il spécifiera comme devant être laissées apparentes, sont adéquates, pertinentes et strictement limitées à ce qui est indispensable à la comparaison entre salariés en tenant compte du ou des motifs allégués de discrimination ;

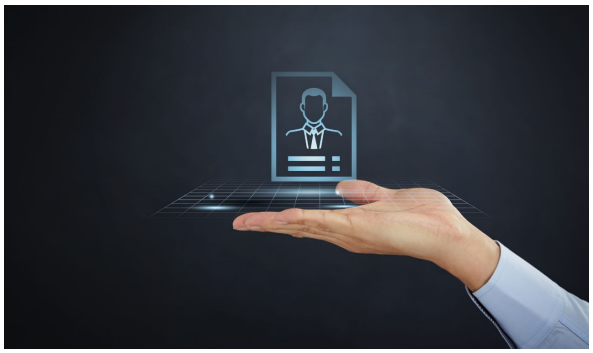
- de faire injonction aux parties (…) de n'utiliser les données personnelles des salariés de comparaison, contenues dans les documents dont la communication est ordonnée, qu'aux seules fins de l'action en discrimination. »

En d'autres termes, le juge prud'homal, saisi d'une demande de communication de documents contenant des données à caractère personnel, dans le cadre d'une action en discrimination, doit :

- vérifier que la communication est nécessaire à l'exercice du droit à la preuve et proportionnée au but poursuivi ;
- au surplus, vérifier quelles mesures sont indispensables à l'exercice du droit à la preuve et proportionnées au but poursuivi, au besoin en cantonnant le périmètre des pièces à communiquer, au regard des faits invoqués et de la nature des pièces sollicitées ;
- ordonner l'occultation des données personnelles non indispensables à l'exercice du droit à la preuve et qui ne sont pas adéquates, pertinentes et strictement limitées à ce qui est indispensable à la comparaison entre salariés ;
- enjoindre les parties à n'utiliser les données personnelles contenues dans les documents qu'aux seules fins de l'action en discrimination.

En l'espèce, la Cour de cassation a estimé que le juge prud'homal n'avait pas procédé aux occultations nécessaires et n'avait pas fait injonction aux parties de n'utiliser les données personnelles qu'aux seules fin de l'action en discrimination. Elle a, en conséquence, cassé l'arrêt d'appel.

Source : ici



LA FOURNITURE SPONTANEE DE DONNEES NE CONSTITUE PAS UN CONSENTEMENT A LEUR TRAITEMENT

Le 26 septembre 2024, la CNIL a sanctionné les sociétés de voyance COSMOSPACE et TELEMAQUE, notamment pour avoir traité des données sensibles, fournies spontanément par les personnes concernées, sans consentement valable.

Des sociétés de voyance traitant des données sensibles

La CNIL a procédé à des contrôles à l'égard des sociétés de voyance en ligne COSMOSPACE et TELEMAQUE, qui ont révélé plusieurs manquements, dont l'un était lié au traitement de données sensibles (orientation sexuelle, état de santé, etc.) communiquées spontanément par les personnes sollicitant une consultation.

Une conception large de la notion d'orientation sexuelle

La CNIL a constaté, au cours de ses contrôles, que les utilisateurs des sites web exploités par COSMOSPACE et TELEMAQUE pouvaient remplir un formulaire ayant pour objet de délivrer une prédiction sur leur compatibilité amoureuse avec une personne de leur choix, permettant ainsi d'en déduire leur orientation sexuelle.

La CNIL a donc considéré cette collecte d'informations comme un traitement de données sensibles, au sens de l'article 9 du RGPD.

Fournir spontanément des données sensibles n'est pas consentir à leur traitement

Outre les données liées à l'orientation sexuelle, collectées via le formulaire en ligne susvisé, les sociétés de voyance traitaient également des données sensibles dans le cadre des consultations réalisées par chat et par SMS.

La CNIL a rappelé que la fourniture de données sensibles spontanément par une personne concernée n'exempte pas le responsable du traitement de s'assurer du respect des conditions posées par l'article 9 du RGPD, à savoir, ici, recueillir le consentement de la personne qui fournit spontanément ses données :

> « *La formation restreinte relève donc, comme elle l'a déjà fait récemment à l'égard d'un autre organisme délivrant des prestations de voyance, que la simple volonté de recevoir ce type de prestation et le fait de livrer spontanément des informations sensibles ne constituent pas un consentement explicite des personnes concernées au traitement de leurs données, et que le responsable de traitement doit mettre à la disposition des personnes auprès desquelles il collecte des catégories particulières de données un moyen permettant de s'assurer qu'elles y consentent de manière explicite par un acte positif clair (CNIL, FR, 8 juin 2023, Sanction, SAN-2023-008, publié).* »

Les deux sociétés, ayant ainsi violé l'article 9 du RGPD, ont été sanctionnées pour traitement de données sensibles illicite.

En raison de l'ensemble des manquements relevés, la CNIL a prononcé :

- une amende administrative de 250.000 euros à l'encontre de COSMOSPACE ;
- une amende administrative de 150.000 euros à l'encontre de TELEMAQUE.

Cette décision doit nous alerter sur la rigueur dont la CNIL fait preuve lorsqu'elle apprécie la notion de « données sensibles » et le respect des règles régissant leur traitement.

Source : ici

DOCTRINE

RGPD

Nos actes quotidiens sont-ils soumis au RGPD ?

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'application du RGPD à des actes relativement banals auxquels se livre une grande majorité de la population.

Si le RGPD s'applique à tous les traitements de données à caractère personnel automatisés ou non, une exception demeure s'agissant des traitements effectués par une personne physique « *dans le cadre d'une activité strictement personnelle ou domestique* »[1].

La règlementation ne définit pas ce type d'activités, mais précise, dans son considérant 18, qu'il s'agit des traitements « *sans lien avec une activité professionnelle ou commerciale* », comme par exemple : « *l'échange de correspondance* », « *la tenue d'un carnet d'adresses* », « *l'utilisation de réseaux sociaux* » et « *les activités en ligne qui ont lieu dans le cadre de ces activités* ».

À la lumière de plusieurs décisions[2], nous avions constaté, dans un article précédent[3], que les autorités de protection des données et la CJUE ont tendance à faire application de la règlementation sur la protection des données chaque fois que le traitement réalisé par un particulier dépasse la sphère strictement privée. En d'autres termes, il est fait application du RGPD si la sphère publique est impactée, soit parce que les données enregistrées concernent des personnes extérieures à la sphère privée de la personne qui réalise le traitement (exemple des caméras qui filment l'espace public), soit parce que les données ont été rendues accessibles à un nombre indéfini de personnes (exemple de la publication de données sur internet, bien qu'enregistrées dans un contexte privé).

Nous avions alors fait le constat d'un champ d'application matériel du RGPD particulièrement large, plus large que nous aurions pu l'imaginer, dès lors qu'il s'applique aussi aux traitements mis en œuvre par les particuliers, et ce chaque fois que ces traitements dépassent le cadre strictement privé de la personne qui en est à l'origine. Tel est notamment le cas de la publication par une personne sur un réseau social d'une vidéo d'une tierce personne se trouvant sur la voie publique, et ce sans le consentement de cette dernière[4].

Des exemples de ce type, nous en rencontrons fréquemment au fil de nos lectures consacrées aux décisions rendues par les autorités nationales de protection des données. Et nous constatons que des actes – bien souvent – en apparence très banals tombent régulièrement sous le coup de la règlementation. En voici quelques illustrations...

Les affaires

En Allemagne, une cliente, qui s'était rendue dans un restaurant, avait, en application de la règlementation en vigueur en Allemagne au moment des faits (période du COVID), renseigné ses coordonnées - dont son numéro de téléphone mobile personnel - sur une fiche dédiée. Le lendemain, cette personne avait eu la surprise d'être contactée sur Messenger par l'un des serveurs.

Elle a déposé une plainte et le serveur a été sanctionné pour avoir détourné les données de leur finalité initiale[5]. Des exemples de ce type sont nombreux. On pense notamment à cet agent de sécurité

qui avait recontacté une personne accusée de vol à l'étalage grâce aux coordonnées recueillies au moment du contrôle en magasin[6] ou encore à cette patiente d'un laboratoire de biologie médicale qui avait été sollicitée sur Instagram, le lendemain de son test, par un membre du personnel de cet établissement[7].

L'usage de caméras dans les espaces publics donne également lieu à quelques situations cocasses. L'un des cas concerne une surveillance vidéo réalisée au moyen d'une caméra sauvage, cachée dans un buisson, qui avait été installée par son propriétaire dans la zone de baignade nudiste d'un lac. La caméra réalisait non seulement des enregistrements vidéos mais également des enregistrements sonores. Son propriétaire a été sanctionné, pour défaut de base légale, par l'autorité allemande de protection des données[8]. Un autre cas concernait un automobiliste qui avait installé dans son véhicule deux caméras (dash-cams) : l'une couvrant la circulation publique à l'avant du véhicule ; et l'autre couvrant l'arrière. Le motif invoqué ? Le conducteur voulait se constituer des preuves en cas d'accident de la route. Considérant qu'*« il n'existe pas de base juridique (...) qui justifierait la légalité de ce traitement de données »*, l'autorité autrichienne de protection des données saisie du dossier a prononcé une sanction à l'encontre de l'automobiliste[9]. En Espagne, le verdict a été similaire s'agissant d'un bailleur qui avait installé une caméra de vidéosurveillance dans le couloir d'un logement qui filmait les parties communes et l'entrée de la chambre de la plaignante, ainsi que l'accès à la salle de bain et à la cuisine[10]. Une amende a également été prononcée à l'encontre d'un individu qui, avec son téléphone mobile, avait pris en photo un groupe de mineurs et des agents de police qui se trouvaient sur la voie publique, puis avait publié les photographies ainsi réalisées sur son compte personnel Facebook[11].

Enfin, un individu, qui avait des vues sur une fille, a été condamné pour avoir installé un AirTag Apple sur le véhicule de cette dernière afin de connaître ses déplacements. L'autorité allemande a estimé que l'exception domestique ne pouvait pas jouer au cas d'espèce et a infligé une amende à quatre chiffres en raison de l'intensité de l'intrusion et de la sensibilité des données[12].

Quelles recommandations ?

Ces cas ne couvrent pas toutes les situations – bien trop nombreuses - dans lesquelles la règlementation sur la protection des données personnelles aurait vocation à s'appliquer... Que penser du skieur équipé d'une caméra GoPro filmant l'intégralité de ses descentes et donc filmant, au passage, des dizaines voire des centaines d'autres skieurs ? Que dire du papa ou de la maman qui dépose un AirTag dans le cartable de son enfant ? Le photographe – amateur ou professionnel – qui shoote des scènes de vie d'inconnus se promenant dans la rue est-il soumis au RGPD ? Le métier de paparazzi est-il vraiment licite en application de cette règlementation ? Peut-on réellement encore publier sur les réseaux sociaux des images prises dans la rue dans lesquelles apparaîtraient d'autres individus n'ayant consenti ni à la photo ni à sa publication ? Quid de la publication d'un selfie réalisé avec une célébrité rencontrée dans une gare ou un aéroport ? On le voit, les situations dans lesquelles le RGPD pourrait s'appliquer sont nombreuses. Méfions-nous !

Alexandre FIEVEE
Avocat associé
Derriennic Associes

Notes

(1) RGPD, article 2.2.c).

(2) CJUE, 6 novembre 2003, C-101/01 ; CJUE, 11 décembre 2014, C-212/13 ; GPDP, 27 avril 2023, n° 9896468 ; Autorité de protection des données belge, 24 novembre 2020, DOS-2019-04412 ; Autorité de protection des données islandaise, 14 juin 2023, affaire n° 2022030544 ; Autorité de protection des données belge, 20 mars 2023, DOS-2022-00945.

(3) « RGPD – Application aux traitements réalisés par des particuliers », Alexandre Fievée, Expertises, septembre 2023, P. 282.

(4) « Diffusion sur les réseaux sociaux d'une vidéo non consentie », Alexandre Fievée, Expertises, octobre 2023, P. 318.

(5) Rapport annuel 2022 du commissaire à la protection des données de la ville de Brême (Allemagne)

(6) Rapport annuel 2023 de l'office bavarois de la protection des données (BayLDA) (Allemagne)

(7) Rapport annuel 2022 du commissaire à la protection des données de la ville de Brême (Allemagne)

(8) Rapport annuel 2023 de l'office bavarois de la protection des données (BayLDA) (Allemagne)

(9) Autorité autrichienne de protection des données (dsb), 27 septembre 2018

(10) Autorité espagnole de protection des données (AEPD), 26 octobre 2023

(11) Autorité espagnole de protection des données (AEPD), 20 mai 2022

(12) Rapport annuel 2023 de l'office bavarois de la protection des données (BayLDA) (Allemagne)

Vous avez envie de vous exprimer sur un sujet qui vous tient à cœur, de partager votre analyse avec la communauté des lecteurs d'Expertises, d'exposer un point de vue différent sur un article déjà publié, de lancer un débat sur un thème émergent, ou simplement de commenter l'actualité du droit du numérique ?

Contactez la rédactrice en chef d'Expertises Sylvie Rozenfeld sr@expertises.info

VU DANS LA PRESSE

« DSIH », OCTOBRE 2024

L'ACHAT EN LIGNE DE MEDICAMENTS NECESSITE-T-IL LE CONSENTEMENT DES CLIENTS AU TRAITEMENT DE LEURS DONNEES DE SANTE ?

Nous savons que la notion de donnée de santé doit être interprétée très largement. Toutefois, dans certaines circonstances, la question se pose de savoir si on est en présence ou non de données concernant la santé. Cette question a été posée à la Cour de Justice de l'Union Européenne (CJUE), qui a dû se prononcer sur le fait de savoir si, lors d'une commande en ligne de médicaments, les éléments nécessaires à leur individualisation doivent s'analyser comme des données de santé.

L'affaire opposait deux pharmaciens allemands. Le premier reprochait au second la commercialisation sur une place de marché en ligne (Amazon), au mépris des règles du RGPD, de médicaments non soumis à prescription médicale. Le non-respect du RGPD résidait, selon le premier pharmacien, dans le fait que le second n'obtenait pas le consentement préalable des clients, personnes concernées, pour le traitement de leurs données de santé (article 9 du RGPD).

Le premier a alors formé un recours en justice contre le second afin qu'il soit mis fin à une telle pratique considérée comme déloyale.

A cette occasion, la juridiction allemande saisie du litige a interrogé la CJUE sur le point notamment de savoir si l'article 9 du RGPD doit être interprété en ce sens que les informations que les clients saisissent lors de la commande en ligne de médicaments - nom, adresse de livraison, éléments nécessaires à l'individualisation des médicaments – constituent des données concernant la santé.

La CJUE a d'abord indiqué que *« lorsque les données sur les achats des médicaments permettent de tirer des conclusions sur l'état d'une personne identifiée ou identifiable »*, elles doivent être considérées comme étant *« des données concernant la santé ».* Il suffit ainsi, a ajouté la Cour, que ces données *« soient de nature à révéler, par une opération intellectuelle de rapprochement ou de déduction, des informations sur l'état de santé de la personne concernée ».*

A cet égard, la juridiction européenne a estimé qu'il importe peu que les médicaments puissent être destinés non pas au client qui réalise la commande mais à des personnes tierces. La CJUE en a conclu que *« les informations que les clients d'un exploitant d'une pharmacie saisissent lors de la commande en ligne de médicaments dont la vente est réservée aux pharmacies sans être soumise à prescription médicale constituent des données concernant la santé (…), même si c'est seulement avec une certaine probabilité, et non avec une certitude absolue, que ces médicaments sont destinés à ces clients »*.

La Cour a précisé enfin que le fait que de telles informations constituent des données de santé ne fait pas obstacle à leur traitement par l'exploitant de la pharmacie, mais à condition que l'une des conditions de l'article 9-2 du RGPD soit respectée, en l'occurrence soit que le client a donné son consentement (article 9-2 a)), soit que le traitement est nécessaire aux fins de la prise en charge sanitaire (article 9-2 h)).

C’est à la juridiction allemande qu’il reviendra de répondre à la question de la licéité de ce traitement, qui, en l’espèce, ne repose pas sur le consentement. Affaire à suivre…

Source : ici

DEUX PHARMACIENS S'ECHARPENT DANS UN LITIGE « RGPD »

La conformité au RGPD requiert des investissements économiques et humains non négligeables. Aussi, quand un professionnel s'affranchit du respect de cette règlementation, il peut en retirer un avantage, par exemple, en proposant des prix plus bas ou des offres plus attractives. Un concurrent pourrait-il se prévaloir d'un manquement au RGPD de ce professionnel pour faire cesser cette pratique et/ou obtenir des dommages et intérêts ? La Cour de Justice de l'Union Européenne (CJUE) a été récemment saisie de cette problématique et a tranché positivement.[1]

L'affaire opposait deux pharmaciens allemands. Le premier reprochait au second la commercialisation, au mépris des règles du RGPD, sur une place de marché en ligne (Amazon) de médicaments non soumis à prescription médicale. Le non-respect du RGPD résidait, selon le premier pharmacien, dans le fait que le second n'obtenait pas le consentement préalable des clients, personnes concernées, pour le traitement de leurs données de santé.

Le premier a alors formé un recours en justice contre le second afin qu'il soit mis fin à une telle pratique considérée comme déloyale.

A cette occasion, la juridiction allemande saisie du litige a interrogé la CJUE sur le point de savoir si ce type d'action en justice était permise par le RGPD.

La CJUE a jugé qu'aucune disposition du RGPD *« n'exclut expressément la possibilité pour le concurrent d'une entreprise d'introduire un recours devant les juridictions civiles contre cette entreprise sur le fondement de l'interdiction des pratiques commerciales déloyales, en raison de la violation alléguée par cette entreprise d'obligations prévues par ce règlement ».* Cette possibilité *« s'ajoute aux voies de recours »* prévues par le RGPD.

La CJUE souligne, en particulier, que cette possibilité de recours *« est de nature à renforcer l'effet utile [du RPGD] et ainsi le niveau élevé de protection des personnes concernées à l'égard du traitement de leurs données personnelles ».*

Il appartiendra alors à la juridiction nationale allemande de vérifier si la violation présumée du RGPD *« pour autant qu'elle soit établie, est également constitutive d'une violation des pratiques commerciales déloyales telle que prévue par la règlementation nationale pertinente »*.

Que peut-on en retenir ?

Le non-respect du RGPD peut être sanctionné sur le terrain des pratiques commerciales déloyales interdites telles que prévues par une loi locale de l'UE.

En France, les juges ont déjà considéré que le non-respect du RGPD peut constituer un acte de concurrence déloyale.

De façon générale, la Cour de cassation a jugé que *« constitue un acte de concurrence déloyale le non-respect d'une réglementation d'une activité commerciale, qui induit nécessairement un avantage concurrentiel indu pour son auteur*[2]*».*

Aussi, tant le Tribunal Judiciaire de Paris[3] que la Cour d'appel de Paris[4] ont admis l'action en concurrence déloyale du fait d'une violation du RGPD, violation permettant nécessairement *« de bénéficier d'un avantage commercial indu ».*

Cette nouvelle décision de la CJUE ajoute une pierre à l'édifice des recours possibles, dans l'Union européenne, contre un concurrent qui ne respecte pas le RGPD.

Un conseil : ne négligez pas votre conformité au RGPD et vérifiez si vos principaux concurrents sont de *« bons élèves »* afin d'envisager, le cas échéant, un recours contre eux…

Source : ici

[1]CJUE, 4 octobre 2024, Affaire C-21/23.

[2]Cass. Com., 17 mars 2021, n°19/10414.

[3]TJ Paris, 15 avril 2022, n°19/12628.

[4]CA de Paris, 9 novembre 2022, n°21/00180.

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

4.000 € 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* » (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 2024/2025 :
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