NEWSLETTER RGPD/DATA

NUMÉRO 69 ● 2025

ACTUALITÉS DU CABINET P. 15

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

SOMMAIRE

ACTUALITÉ

- Quand le sexe ressenti est une donnée plus exacte que le sexe réel. **p.2**
- Pas d'exception au droit à l'effacement si le recours en justice est « improbable ». **p.3**
- Vous êtes DPO ? Devenez avocat ! **P.4**
- Le chiffre d'affaires du groupe comme base de calcul de l'amende RGPD. **P.5**

VU DANS LA PRESSE

- La liberté expression menacée par le RGPD ? **p.7**
- Quand le RGPD fait échec au contrat. **p.11**
- Conformité et sécurité des dossiers médicaux : ce que propose la CNIL. **p.13**

QUAND LE SEXE RESSENTI EST UNE DONNEE PLUS EXACTE QUE LE SEXE REEL

Dans un arrêt du 13 mars 2025, la Cour de justice de l'Union européenne a estimé que la donnée relative au sexe de naissance devait être corrigée en cas de transition de genre, même en l'absence de preuve d'opération chirurgicale, et même si aucune disposition de droit national ne reconnait le changement d'identité de genre.

Une demande de rectification du genre, sans preuve d'opération chirurgical

L'autorité hongroise en charge de l'asile a reconnu le statut de réfugié à une femme de nationalité iranienne, en raison de sa transidentité.

Faute de produire un document attestant d'une opération chirurgicale de changement de sexe, cette personne a été enregistrée, dans le registre de l'asile, en tant que femme (son sexe de naissance) plutôt qu'en tant qu'homme (son « *identité de genre* »).

La femme, estimant devoir être inscrite en tant qu'homme, a formé, sans succès, une demande de rectification auprès de l'autorité en charge de l'asile. Dans ce contexte, elle a saisi la justice pour contester cette décision de rejet.

Les juridictions hongroises ont saisi la Cour de justice de l'Union européenne (CJUE) de la question préjudicielle suivante :

Le droit de rectification oblige-t-il l'autorité en charge de la tenue d'un registre à rectifier les données relatives au genre de la personne concernée, lorsque cette dernière estime que son genre a changé, alors (i) que le droit national ne reconnait pas le changement d'« *identité de genre* » et (ii) que la personne concernée ne fournit pas de preuve de traitement chirurgical de réassignation sexuelle ?

Une rectification due y compris en l'absence de reconnaissance du changement de genre par le droit national

Pour la CJUE, il ressort des circonstances du traitement que le registre de l'asile semble traiter « *l'identité de genre vécue par cette personne* », plutôt que « *celle qui lui aurait été assignée à la naissance* ».

Ayant reconnu la transidentité de la personne concernée, l'autorité hongroise en charge de l'asile aurait dû en tirer les conséquences et inscrire cette personne sous son « *identité de genre* », étant précisé que l'absence de reconnaissance du changement d'« *identité de genre* » par le droit hongrois est inopérante (« *un État membre ne saurait se prévaloir de dispositions de droit national spécifiques (…) pour faire obstacle au droit de rectification* »).

Une rectification due y compris en l'absence de preuve d'opération chirurgicale

Enfin, pour la CJUE, subordonner l'exercice du droit de rectification de l'identité de genre à la production d'une preuve de traitement chirurgical de réassignation sexuelle « *ne répond pas à l'exigence selon laquelle le droit d'un État membre ne peut limiter la portée du droit prévu à l'article 16 du RGPD que par la voie de mesures législatives* ».

Or, en l'espèce, aucune mesure législative n'a été adoptée sur ce point, l'absence de procédure de reconnaissance de la transidentité par le droit hongrois ne constituant pas, pour la CJUE, « *une mesure législative afférente aux exigences de preuve applicables quant à la rectification des données relatives à l'identité de genre des personnes inscrites au registre de l'asile* ».

Source : ici

PAS D'EXCEPTION AU DROIT A L'EFFACEMENT SI LE RECOURS EN JUSTICE EST « IMPROBABLE »

Le tribunal régional supérieur de Karlsruhe a considéré qu'un responsable du traitement ne peut pas s'opposer à une demande d'effacement au motif que les données sont nécessaires « à la constatation, à l'exercice ou à la défense de droits en justice », si le recours en justice est « improbable ».

La demande d'effacement de données dont le traitement n'est plus nécessaire

Des pirates se sont introduits frauduleusement sur le compte d'un utilisateur d'un réseau social et y ont publié des fichiers pédopornographiques.

Alerté, le gestionnaire du réseau social a temporairement bloqué le compte de l'utilisateur le temps (i) d'enquêter sur les faits et (ii) de se prononcer sur une éventuelle sanction de l'utilisateur pour non-respect des conditions générales d'utilisation de la plateforme.

Le titulaire du compte piraté a indiqué au gestionnaire du réseau social qu'il n'était pas à l'origine de la publication des fichiers pédopornographiques et a demandé le déblocage de son compte.

Le gestionnaire du réseau social a rétabli le compte mais a conservé l'information selon laquelle ce compte a fait l'objet d'un blocage temporaire et que des publications y ont été supprimées.

L'utilisateur du réseau social a saisi la justice allemande afin, notamment, d'obtenir la suppression de ladite information conservée par le gestionnaire du réseau social.

Pour ce faire, l'utilisateur du réseau social se fondait sur l'article 17§1.a) du RGPD selon lequel la personne concernée a le droit d'obtenir du responsable du traitement l'effacement de ses données à caractère personnel lorsque les données *« ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées* ».

L'impossibilité, pour le gestionnaire du réseau social, de s'opposer à l'effacement des données

Pour sa défense, le gestionnaire du réseau social s'opposait à la suppression des données relatives à l'incident en invoquant l'article 17§3.e) du RGPD qui dispose que le droit à l'effacement ne s'applique pas dans la mesure où le traitement est nécessaire « *à la constatation, à l'exercice ou à la défense de droits en justice* ».

Le tribunal a cependant indiqué que cet article du RGPD n'était pas invocable en l'espèce. En effet, selon le tribunal, les données personnelles de l'utilisateur avaient été collectées et traitées à la suite d'un incident afin (i) d'enquêter sur les faits et (ii) de se prononcer sur une éventuelle sanction mais puisque le gestionnaire du réseau social a conclu que les faits litigieux n'étaient pas le fait de la personne concernée, a rétabli le compte et n'a prononcé aucune sanction, les raisons qui ont motivé le traitement des données ont disparues et le traitement des données à caractère personnel n'est plus « nécessaire ». En outre, le tribunal a indiqué que, bien que l'existence d'un recours en justice d'un tiers ou de l'utilisateur est une possibilité, ce recours est « improbable », de sorte qu'il n'est pas possible de s'opposer à la suppression des données.

Compte tenu de ce qui précède, le tribunal a notamment ordonné au gestionnaire du réseau social de supprimer de ses bases de données les données relatives à l'existence d'un blocage temporaire et à l'existence de publications supprimées.

Source : ici

VOUS ETES DPO ? DEVENEZ AVOCAT

Par un arrêt du 19 mars 2025, la Cour de cassation a considéré que les tâches réalisées par une DPO étaient assimilables à celles réalisées par un juriste d'entreprise, au regard des exigences liées à la dispense de formation et de diplôme pour accéder à la profession d'avocat.

Une dispense refusée à la DPO

Une DPO a demandé son inscription au tableau de l'Ordre des avocats, au titre de la dispense de formation et de diplôme prévue pour les juristes ayant exercé, pendant au moins 8 ans, une activité exclusivement au sein d'un service spécialisé de l'entreprise, chargé des problèmes juridiques de cette entité.

Cette demande lui a été refusée par l'Ordre, au motif que cette personne exerçait des fonctions, non pas de juriste, mais de DPO et de « *responsable conformité* », et était rattachée à la direction générale et non à la direction juridique de son entreprise.

La DPO a saisi la justice afin de contester cette décision.

Les fonctions de DPO peuvent s'assimiler à celles de juriste d'entreprise

Pour déterminer si la DPO peut se prévaloir de la dispense, la Cour de cassation a apprécié la nature des actions réalisées par celle-ci. Elle a ainsi noté, outre les tâches liées à ses fonctions de responsable conformité, les activités suivantes :

- La rédaction de « *quatre fascicules en relation avec le règlement général sur la protection des données (RGPD) » ;*
- Le renseignement d'autres collaborateurs sur « *les règles applicables en cette matière [le RGPD]* »
- *Son intervention « dans l'évolution du contrat de collaboration informatique avec les sous-traitants ».*

Selon la Cour de cassation, ces éléments démontrent que la DPO exerçait « *des activités de juriste d'entreprise »* et a, en conséquence, décidé que la DPO pouvait bien se prévaloir de la dispense prévue pour exercer la profession d'avocat.

Source : ici

LE CHIFFRE D'AFFAIRES DU GROUPE COMME BASE DE CALCUL DE L'AMENDE RGPD

La Cour de Justice de l'Union Européenne s'est récemment positionnée sur un sujet crucial en matière de RGPD : comment calculer le montant de l'amende pour une entité faisant partie d'un groupe de sociétés ? Doit-on tenir compte du chiffre d'affaires de l'entité objet de la sanction ou celui du groupe auquel elle appartient ?

L'affaire opposait une société danoise, exploitante d'une chaine de magasins et appartenant à un groupe de sociétés, à l'autorité de protection des données danoise. Cette dernière reprochait à la société un manquement au RGPD relativement à la conservation de données personnelles de ses clients. En conséquence, l'autorité a prononcé contre la société une amende administrative d'un montant équivalent à environ à 200.000 euros, montant calculé non seulement au regard du chiffre d'affaires réalisé par la société (équivalent à environ 280.000 euros), mais aussi à celui réalisé par le groupe auquel elle appartient (880.000 euros). Contestant une telle règle de calcul, la société a formé un recours. La juridiction de 1ère instance a réduit le montant de l'amende à 10.000 euros en considérant notamment qu'il n'y avait pas lieu de tenir compte du chiffre d'affaires du groupe. L'autorité de protection des données a remis en cause une telle position et fait appel de cette décision. C'est dans ce cadre que la CJUE a été saisie de la problématique.

Pour mémoire, le RGPD prévoit à son article 83 (§1 et §2) que l'autorité de protection des données doit veiller à ce que l'amende soit effective, proportionnée et dissuasive. A cette fin, l'autorité doit tenir compte de plusieurs éléments tels que la nature, la gravité et la durée de la violation, le nombre de personnes concernées affectées, le fait que la violation a été commise délibérément ou par négligence, etc. A cela s'ajoute la condition de la « *capacité économique réelle ou matérielle* » de l'organisme objet de la sanction[1].

Aussi, il est prévu à ce même article 83 (§4 et §6) que, pour certains manquements d'une particulière gravité, l'amende prononcée par une autorité de protection des données peut aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise.

Mais qu'entend-on par « entreprise » ?

La CJUE a jugé, à la lumière du considérant 150 du RGPD, qu'il faut entendre la notion d' « entreprise » comme celle définie aux articles 101 et 102 du Traité sur le Fonctionnement de l'Union Européenne (TFUE). Il s'agit donc d' « *une unité économique* », à avoir « *une organisation unitaire d'éléments personnels, matériels et immatériels poursuivant de façon durable un but économique déterminé* » et ce, « *même si, du point de vue juridique,* [elle] *est constituée de plusieurs personnes physiques ou morale* ».

La CJUE en a tiré deux conséquences :

- Le montant maximal de l'amende administrative encouru par une entité, « *qui est ou fait partie d'une entreprise* », est calculé sur la base d'un pourcentage du chiffre d'affaires annuel mondial total de l'exercice précédent de l'« entreprise » concernée, et ainsi du groupe auquel appartient l'entité ;
- Le montant final de l'amende, lequel doit être effectif, proportionné et dissuasif, est déterminé en tenant également compte de cette notion d' « entreprise », et donc, encore une fois, du groupe auquel appartient l'entité destinataire de l'amende.

[1] En ce sens, CJUE 5 décembre 2023, C-807/21.

Que faut-il en retenir ?

Toute société faisant partie d'un groupe de sociétés et répondant aux critères de l'unité économique telle que définie par les règles de la concurrence (articles 101 et 102 du TFUE) s'expose à un risque d'amende d'un montant potentiellement conséquent dans la mesure où il est fixé notamment au regard du chiffre d'affaires réalisé par le groupe.

Il est donc plus que jamais temps pour les entreprises de s'assurer de leur conformité RGPD, avec l'appui de leur groupe, le cas échéant.

Source : ici

VU DANS LA PRESSE

« EXPERTISES », MARS 2025

INTERVIEW

ALEXANDRE FIÉVÉE

La liberté d'expression menacée par le RGPD ?

Surtout depuis internet, deux visions de la liberté d'expression opposent les Etats-Unis à l'Europe où celle-ci peut être limitée pour des motifs de protection de droits de la personnalité visant à éviter toute diffamation, discrimination ou atteinte excessive à la vie privée d'autrui. Depuis peu, le RGPD est invoqué par des personnes pour contester la publication d'articles les concernant. Et des autorités de contrôle européennes leur ont donné gain de cause. Les médias ne savent pas toujours que le RGPD s'applique à eux, même s'ils bénéficient de quelques dérogations. Le grand public non plus d'ailleurs. Alexandre Fiévée, avocat spécialiste en droit de la protection des données personnelles, nous dit dans quelle mesure le RGPD peut imposer des limites à la libre parole des journalistes mais aussi des particuliers.

EXPERTISES MARS 2025 11

Sylvie Rozenfeld : Internet a permis à tout le monde de s'exprimer et de diffuser sa parole librement dans des commentaires, des blogs ou sur les réseaux sociaux. Comme la presse, les personnes bénéficient de la liberté d'expression. Mais ce droit n'est pas absolu. Une des limites récemment opposée à la liberté d'expression est la protection des données personnelles. L'article 85 du RGPD prévoit que les États membres concilient, par la loi, le droit à la protection des données à caractère personnel et le droit à la liberté d'expression et d'information, y compris le traitement à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire et qu'ils peuvent adopter des dérogations et des exemptions. Avant d'aborder la jurisprudence de la Cour de justice de l'UE et des autorités de contrôle en matière de données personnelles, j'aimerais qu'on commence sur une considération générale sur la réalité de la menace du RGPD sur la liberté d'expression.

Christophe Bigot considère qu'on assiste à une expansion hégémonique du droit des données personnelles au détriment de la liberté d'expression alors que ces droits « *ne sont ni absolus ni hiérarchisés entre eux, étant d'égale valeur* ». Selon lui, ce sont deux systèmes de droit reposant sur des philosophies radicalement différentes qui posent la question de leur compatibilité. Y-a-t-il une antinomie fondamentale entre la liberté d'expression, qui se fonde sur des possibilités illimitées de rassemblement et de circulation des informations et la protection des données à caractère personnel qui exige au contraire (...) de strictes limitations afin d'assurer le respect de la vie privée ?

Alexandre Fiévée : La règlementation en matière de protection des données personnelles ne limite pas la liberté d'expression. Au contraire, l'article 85 donne même la possibilité à chaque Etat membre de prévoir par la loi un régime dérogatoire pour les traitements réalisés à des fins journalistiques. Il ne s'agit donc pas de restreindre la liberté d'expression mais de à la protection des données personnelles. C'est dans ce cadre que le législateur français a ainsi écarté, pour les traitements journalistiques, certains principes du RGPD (principe de transparence, principe d'interdiction de traiter des données sensibles mais aussi des données relatives aux condamnations, etc.) et plusieurs droits reconnus aux personnes concernées (droits d'accès, de vérification, etc.).

« Les traitements réalisés par des particuliers sont soumis au RGPD, dès l'instant qu'ils débordent dans la sphère publique. »

La liberté d'expression s'applique aussi aux particuliers qui s'expriment sur leur site, blog ou sur les réseaux sociaux. Et l'article 2.2. c) prévoit que le RGPD ne s'applique pas aux traitements effectués par une personne physique dans le cadre d'une activité strictement personnelle ou domestique. Où se situe la frontière à partir de laquelle le RGPD s'applique ?

On a longtemps pensé, et certains le pensent encore, que la règlementation sur la protection des données personnelles ne s'applique pas aux traitements réalisés par des particuliers car les traitements dits « *domestiques* » sont exclus du champ d'application du RGPD. Or, la CJUE, tout comme certaines autorités nationales de contrôle dans l'UE, ont eu l'occasion de préciser cette notion de traitement « *domestique* » et ont considéré qu'elle devait se limiter aux traitements réalisés dans le cadre de la sphère privée de l'individu. Dès qu'ils débordent dans la sphère publique, ils sont soumis au RGPD. Prenons l'exemple d'un dispositif de vidéosurveillance installé à l'entrée d'une propriété privée. Si la caméra est orientée, ne serait-ce qu'en partie, vers l'espace public et si elle filme, par voie de conséquence, des personnes qui sont extérieures à la propriété, il ne s'agit pas d'un traitement domestique, mais d'un traitement soumis au RGPD avec toutes les conséquences qui en découlent. Seconde situation dans laquelle le RGPD s'applique : les données, bien que collectées par un individu dans un cercle privé, sont diffusées par celui-ci à un nombre indéfini de personnes, par exemple sur les réseaux sociaux. Dans les deux exemples susvisés, bien que les traitements soient réalisés par des particuliers, ils sont soumis au RGPD.

Mais si vous diffusez les données personnelles d'un tiers sur un réseau social sur un compte privé, le traitement, soumis au RGPD, est-il licite ?

Se pose la question de la base légale du traitement. Et la seule qui semble pouvoir s'appliquer dans cette situation est celle du consentement de la personne concernée, contrairement au journaliste, qui dans le cadre d'un article dans lequel il mentionnerait des données relatives à un tiers, pourrait, lui, se prévaloir d'un intérêt légitime. Cette exigence du consentement comme base légale peut s'avérer problématique. Prenons l'exemple du selfie réalisé par un particulier avec une personnalité publique croisée dans la rue et mis en ligne dans les minutes qui suivent. On pourrait considérer que la personnalité a donné son consentement pour le selfie puisqu'elle se met devant la caméra ou le smartphone pour la captation de son image. Mais a-t-elle donné son consentement pour la diffusion de son image sachant que le RGPD impose que le consentement soit libre, éclairé, spécifique et univoque et donc non-implicite ?

Le RGPD avait pour objectif d'harmoniser la protection des données personnelles dans l'UE. Mais par exemple sur la conciliation de ce droit avec la liberté d'expression, le législateur européen s'est déchargé du problème sur les Etats membres prévoyant qu'ils peuvent adopter des dérogations et des exemptions à l'application du RGPD. En France, l'article 80 de la loi de 1978 modifiée prévoit l'application de dérogations à certains articles de la LIL aux traitements mis en œuvre aux fins d'expression universitaire, artistique ou littéraire et d'exercice à titre professionnel, de l'activité de journaliste.

L'exception relative à l'exercice de la liberté d'expression retenue par le législateur français limite ainsi les dérogations à la seule pratique du journalisme exercée à titre professionnel. Qu'entend-on par « *traitement réalisé à des fins journalistiques* » ? Est-ce réservé à la presse ? Quand peut-on considérer qu'une publication en ligne entre dans le champ de l'exception de journalisme ?
La loi Informatique et libertés ne définit pas le traitement réalisé aux fins d'exercice professionnel de l'activité de journaliste. On pourrait considérer, en application de l'article L.711-3 du code du travail, qu'il s'agit du traitement effectué par une personne qui a pour activité principale, régulière et rétribuée, l'exercice de la profession de journaliste dans une ou plusieurs entreprises de presse, publications quotidiennes et périodiques ou agences de presse et qui en tire le principal de ses ressources. Ainsi le traitement réalisé par un particulier, qui n'est pas journaliste professionnel, n'entre pas dans le cadre du régime dérogatoire prévu par l'article 80 de la loi Informatique et libertés. Il ne peut donc pas se prévaloir des exceptions telles que celles liées aux traitements des données sensibles ou des condamnations.

« Désormais on pourra invoquer le principe de minimisation à l'encontre du journaliste. »

La personne qui conteste la publication d'un contenu la concernant peut se fonder sur une infraction de presse. Avec le RGPD, c'est donc un nouveau fondement que peut invoquer une personne opposée à la publication de données la concernant.

Jusqu'à présent, pour contester la licéité d'un contenu, la personne pouvait invoquer l'injure, la diffamation ou encore l'atteinte à sa vie privée. Désormais avec le RGPD, elle pourra invoquer à l'encontre du journaliste le principe de minimisation. On a vu ce cas de figure notamment en Espagne, dans une affaire qui concernait un site d'information qui avait publié un article sur le caractère viral d'une vidéo diffusée sur le compte Twitter d'un tiers. L'article en question avait publié le nom de la personne concernée et une capture d'écran de la vidéo ainsi qu'un lien vers cette dernière, sans l'autorisation de la personne figurant sur cette vidéo alors qu'elle était identifiable par sa voix et son image. Cette dernière a porté plainte auprès de l'autorité de contrôle espagnole qui a considéré que, bien que le site soit une publication de presse, il restait soumis au RGPD. En publiant le nom de la personne, sa photographie sans la flouter et en diffusant sa voix sans la maquiller, le site n'a pas respecté le principe de minimisation des données car il aurait pu publier cet article sans avoir à communiquer autant de données personnelles. L'autorité espagnole va plus loin en disant que la circonstance selon laquelle le site n'était pas à l'origine de la diffusion de la vidéo est indifférente et celle selon laquelle la personne concernée serait peut-être à l'origine initialement de la publication de la vidéo avant qu'elle soit diffusée sur le compte Twitter est également indifférente. La personne a la maîtrise de ses données et, elle seule, est en mesure de décider des conditions dans lesquelles ses données peuvent être utilisées.

Est-ce que ça ne limite pas la liberté d'expression ?
Je ne pense pas que le RGPD la limite. On pourrait même considérer que le principe de minimisation, en ce qu'il améliore la qualité de l'information, renforce le droit à l'information.

Le droit à l'oubli ou droit à l'effacement, qui a fait l'objet de plusieurs arrêts importants se pose de manière particulièrement sensible pour la presse. Ce droit ne fait pas partie des exceptions prévues par la loi. Quelle est la position de la CJUE en la matière ?
Le législateur français a, s'agissant des traitements journalistiques, écarté au bénéfice des personnes concernées plusieurs droits (droits d'accès, de rectification, et le droit à la limitation des traitements), mais il n'a pas touché au droit à l'effacement (ou droit à l'oubli) ni au droit d'opposition. N'importe quelle personne peut donc exercer ces droits à l'égard de n'importe quel média. Il appartient donc au juge de concilier le droit à la protection des données et la liberté d'expression. Le droit à l'oubli, pour répondre à votre question, a d'abord été appliqué aux moteurs de recherche, sans que cela ait un impact sur le contenu de la publication initiale. Aujourd'hui, ça va beaucoup plus loin puisque la CJUE et la Cour européenne des droits de l'homme (CEDH) reconnaissent la possibilité à la personne concernée d'exercer son droit à l'effacement directement à l'encontre de l'éditeur du contenu litigieux. À titre d'exemple, la CJUE a demandé à l'éditeur d'un contenu litigieux d'introduire une métabalise « *no-index* » dans l'entête du contenu HTLM de la page afin d'empêcher les moteurs de recherche d'indexer cette page de sorte qu'elle n'apparaisse pas dans les résultats de recherche. La CEDH a, quant à elle, demandé à l'éditeur que l'article litigieux en version numérique soit anonymisé et ce, pour préserver la vie privée du requérant.

Comment une publication de presse ou un site d'informations peut-il avoir une politique conforme au RGPD en la matière ?
Les médias ne savent pas toujours que le RGPD s'applique à eux. Le grand public non plus d'ailleurs. Et, à ma connaissance, la Cnil n'a pas rendu de décision ni publié d'articles sur cette problématique visant à concilier le droit à la protection des données personnelles et la liberté d'expression. Le journaliste doit avoir en tête que, si certains principes ne lui sont pas applicables (exemple : le principe de limitation de la durée de conservation des données), d'autres le sont, comme le principe de minimisation.

Le RGPD s'applique-t-il aussi aux personnes interviewées ?
Très bonne question. En effet, le RGPD va concerner le traitement réalisé par le journaliste mais aussi celui réalisé par la personne interviewée qui peut être amenée à évoquer un tiers et des données le concernant, simplement en racontant une histoire, une anecdote ou une affaire déterminée. Dans ce cas, le règlement s'applique. En Italie, une députée avait commis des infractions au code de la route et avait fait l'objet de plusieurs

contraventions. Elle avait souhaité avoir des informations sur le dispositif de contrôle mis en place par la commune et avait demandé au maire de bien vouloir l'accompagner au bureau du service de police. Sur place, l'agent avait répondu aux questions de la députée devant le maire qui ainsi avait été informé de tous détails. La députée a, par la suite, rendu publique cette affaire. Dans le cadre d'une interview, le maire a été interrogé sur cette affaire et a communiqué les informations dont il avait connaissance. La députée n'a pas apprécié la divulgation de ces informations par le maire et a déposé une plainte auprès de l'autorité de contrôle. Celle-ci a considéré le traitement comme illicite pour défaut de base légale, car le maire n'avait pas eu le consentement de la députée pour divulguer de telles informations ; le maire n'étant pas journaliste, il ne pouvait pas invoquer son intérêt légitime. L'autorité de contrôle a estimé comme indifférent le fait que l'information ait été rendue publique par la députée, avant que le maire ne communique dessus. Pourquoi ? Car la personne concernée a seule le pouvoir de décision sur le traitement de ses données personnelles !

« Le RGPD concerne le traitement réalisé par le journaliste mais aussi celui réalisé par la personne interviewée qui peut être amenée à évoquer un tiers et des données le concernant. »

Et la responsabilité du directeur de la publication ?

C'est un autre sujet. Dans l'affaire susvisée, la plainte n'avait pas été déposée contre le média mais contre l'interviewé. Ce cas de figure n'est pas isolé. Récemment, un directeur sportif a été interviewé et a expliqué la méforme de son coureur emblématique en faisant état de son mode de vie. Il a évoqué ses habitudes en dehors de l'entraînement, le rôle joué par sa femme, etc. Le fait de se répandre ainsi dans les médias, pourrait être problématique par rapport au RGPD, et à l'exigence de consentement. Le règlement européen s'applique dans beaucoup plus de situations qu'on pourrait imaginer.

Quid de la publication sur les réseaux sociaux ?

Il n'y a pas, à ma connaissance, de décision de la Cnil concernant la publication sur les réseaux sociaux par des particuliers de contenus illicites au regard du RGPD. On a eu le cas, en revanche, à l'étranger. Je pense notamment à cet individu qui s'est fait sanctionner par l'autorité de contrôle espagnole. L'histoire est la suivante : alors qu'il était dans son véhicule, son attention a été attirée par une jeune fille qui titubait sur le trottoir. Il trouvait la scène drôle, alors il l'a filmée et a diffusé la vidéo sur les réseaux sociaux. La vidéo est devenue virale. La fille s'en est rendue compte et a déposé plainte auprès de l'autorité de contrôle espagnole. Le particulier, qui a filmé et diffusé la vidéo, a invoqué le traitement domestique. Mais il n'a pas été suivi par l'autorité de contrôle qui a estimé qu'il avait dépassé la sphère privée. D'abord, il a collecté l'image d'une fille qui se trouvait sur la voie publique mais en plus il a diffusé la vidéo à un nombre indéfini de personnes. La fille n'ayant pas donné son consentement, les traitements étaient dépourvus de base légale et l'individu a été sanctionné.

La plupart des réseaux sociaux sont américains. Or, l'administration Trump a demandé à trois membres de la Privacy and Civil Liberties Oversight Board de choisir entre démissionner ou être démis de leur fonction. Est-ce que cette décision qui empêcherait cet organisme de fonctionner impacterait le Data Privacy Framework ? Quelles conséquences pour nous Européens ?

Ce comité de surveillance de la vie privée et des libertés civiles est indépendant et il est chargé de superviser la communauté du renseignement américain. Son rôle de surveillance a été un élément important des négociations du Data Privacy Framework, aidant les Etats-Unis à démontrer leur capacité à fournir un niveau de protection des données essentiellement équivalent à celui des données transférées depuis l'UE. On ne sait pas si Donald Trump va pourvoir à des remplacements. Cela pose un problème de quorum et de fonctionnement de ce comité qui est composé de quatre membres. Les trois sommés de démissionner sont démocrates et le seul membre restant est républicain. Si cette démarche ne remet pas en question le DPF, il y a un risque de remise en cause probable du cadre juridique du DPF par la CJUE ou la Commission qui pourront l'invalider. Dans ce cas, on se retrouverait dans la situation antérieure au DPF avec la nécessité de signer des clauses contractuelles types complétées de mesures techniques et organisationnelles visant à sécuriser les transferts de données vers les Etats-Unis.

Propos recueillis par
Sylvie ROZENFELD

DOCTRINE

RGPD

Quand le RGPD fait échec à l'exécution du contrat

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 de contrôle nationales au niveau européen et les juridictions européennes. Ce mois-ci, il se penche sur la question de savoir si le RGPD peut faire obstacle à l'exécution d'un contrat entre un distributeur et un diffuseur, auquel la personne concernée n'est pas partie.

Un traitement de données personnelles doit reposer sur une des six bases légales visées à l'article 6, paragraphe 1 du RGPD. À défaut, le traitement est considéré comme illicite. Les six bases légales sont : (a) le consentement (la personne concernée a consenti au traitement de ses données) ; (b) le contrat (le traitement est nécessaire à l'exécution ou à la préparation d'un contrat avec la personne concernée) ; (c) l'obligation légale (le traitement est imposé par un texte légal) ; (d) la mission d'intérêt public (le traitement est nécessaire à l'exécution d'une mission d'intérêt public) ; (e) l'intérêt légitime (le traitement est nécessaire à la poursuite d'intérêts légitimes de l'organisme qui traite les données) ; (f) la sauvegarde des intérêts vitaux (le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée, ou d'un tiers). La Cnil rappelle régulièrement que le RGPD « *ne crée pas de hiérarchie entre les différentes bases légales* »[1] et explique, à cet égard, que le consentement ne prévaut pas sur les autres bases légales : « *La base légale appropriée doit être déterminée par le responsable du traitement de manière adaptée à la situation et au type de traitement, au cas par cas* »2.

Ainsi lorsqu'un traitement de données personnelles est réalisé dans le cadre de l'exécution d'un contrat auquel la personne concernée est partie, ce traitement a pour base légale l'exécution du contrat (article 6, paragraphe 1, b)), à condition toutefois, précise la Cnil, que « *le traitement soit objectivement nécessaire à l'exécution d'un contrat entre l'organisme traitant les données et les personnes concernées* »[3].

L'autorité française de protection des données donne l'exemple suivant : « *une personne procède à des achats en ligne et souhaite payer par carte bancaire et se faire livrer les produits à son domicile. Il est dès lors nécessaire pour le site marchand en ligne de traiter les données de paiement et l'adresse de livraison de son client : le traitement de ces données vise uniquement l'exécution du contrat conclu avec la personne concernée et les données traitées sont limitées à celles qui sont nécessaires à cette exécution. Le traitement par l'organisme de ces informations peut donc se fonder sur la base légale "contrat".* »

L'application de cette base légale ne devrait pas, dans la pratique, poser de difficulté. Et pourtant...

L'affaire[4]

Une jeune femme a été alertée par un ami au sujet de la diffusion sur le web d'une vidéo pour adultes dans laquelle elle apparaissait. Selon elle, la diffusion de cette vidéo portait atteinte à la réglementation sur la protection des données personnelles. Elle a déposé une plainte auprès de l'autorité espagnole de contrôle, l'AEPD. Selon l'éditeur du site litigieux, la diffusion de la vidéo était parfaitement licite, dans la mesure où la plaignante avait signé un contrat avec un producteur autorisant ce dernier notamment à céder son image à des tiers. C'est dans ce cadre que le producteur avait conclu un contrat avec un tiers, qui avait, lui-même, cédé les droits au défendeur pour l'exploitation en ligne de la vidéo.

Malgré ce cadre contractuel non contesté en l'espèce, l'AEPD a donné gain de cause à la plaignante, considérant que le traitement de l'image de cette dernière par l'éditeur du site litigieux ne reposait sur aucune base légale : « *Le traitement (...) ne peut être fondé sur l'article 6, paragraphe 1, b) du RGPD, car celui-ci exige expressément que le traitement soit nécessaire à l'exécution d'un contrat auquel la personne concernée est partie, ce qui n'est pas le cas en l'espèce* ». En effet, la plaignante, bien que signataire du contrat initial avec le producteur, n'était pas partie au contrat dont se prévaut le défendeur. Le défendeur ne pouvait pas d'avantage invoquer le consentement de la plaignante pour justifier la licéité du traitement, car « *aucun consentement spécifique n'a été obtenu de la part de [la jeune femme] pour autoriser le traitement de ses données* ». L'AEPD ajoute qu'« *aucune information n'a été fournie à [la plaignante] quant à la finalité spécifique, explicite et légitime du traitement des données* ».

Partant, l'autorité espagnole de protection des données a condamné l'éditeur du site web au paiement d'une amende administrative de 10 000 euros et à prendre les mesures nécessaires pour que l'image de la plaignante ne soit plus traitée ni diffusée.

Quelles recommandations ?

Cette décision est très surprenante dans la mesure où la plaignante avait autorisé, dans le contrat initial conclu avec le producteur, l'exploitation de son image par des tiers, traitement indispensable à l'exécution de ce contrat et des autres contrats conclus en application du premier. Par conséquent, il n'était pas nécessaire qu'elle soit partie à tous les contrats. Exiger qu'elle signe tous les contrats n'aurait pas de sens, compte tenu des termes très clairs du premier contrat. Exiger qu'elle donne son consentement « *RGPD* » à chaque cessionnaire n'aurait pas plus de sens. Par ailleurs, une telle base légale - le consentement – mettrait sérieusement en difficulté les distributeurs et diffuseurs qui seraient contraints, malgré les termes des contrats, de cesser l'exploitation de l'image de la personne concernée sur simple demande de cette dernière qui déciderait discrétionnairement – comme l'y autorise le RGPD – à retirer son consentement.

Alexandre FIÉVÉE
Avocat Associé
DERRIENNIC ASSOCIES

Notes

(1) https://www.cnil.fr/fr/les-bases-legales/liceite-essentiel-sur-les-bases-legales

(2) https://www.cnil.fr/fr/les-bases-legales/liceite-essentiel-sur-les-bases-legales

(3) https://www.cnil.fr/fr/les-bases-legales/contrat

(4) AEPD, EXP202300016, 27 janvier 2025.

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

CONFORMITE ET SECURITE DES DOSSIERS MEDICAUX : CE QUE PROPOSE LA CNIL

La CNIL vient de publier un projet de recommandation dédié au Dossier patient informatisé (DPI), soumis à consultation publique. Que faut-il en retenir ? A quoi devons-nous nous attendre ?

Pourquoi ce projet de consultation ?

Plusieurs raisons expliquent l'initiative de la CNIL.

Tout d'abord, le fait que le Dossier patient informatisé (DPI) contient un volume significatif de données sensibles, en ce qu'il centralise l'ensemble des données des patients pris en charge au sein d'un établissement de santé.

Ensuite, parce que ces organismes sont souvent victimes de violations de données (196 notifications émanant des centres hospitaliers, en 2024) et que les conséquences peuvent être considérables, en cas notamment de cyberattaques, pour la santé des patients (blocage complet du SI de plusieurs établissements).

Enfin, parce que la CNIL connaît les difficultés que rencontrent les établissements de santé à assurer de manière effective la confidentialité des données et le respect du secret médical, eu égard notamment aux règles d'habilitations et d'accès à un dossier patient en vigueur au sein de l'organisme.

Quel est son objectif ?

Selon la CNIL, il s'agit « *compte tenu de ces constats et pour accompagner l'ensemble des établissements de santé* », d'élaborer « *un document consolidant les règles applicables au DPI ainsi que ses recommandations juridiques et techniques* ».

Que faut-il en retenir ?

Ce document de 47 pages se compose de 15 fiches.

En bref :

- Il ne s'adresse qu'aux traitements mis en œuvre par un établissement de santé (défini à l'article L. 6111-1 du Code de la santé publique (« CSP »)), à des fins d'enregistrement et de conservation des données personnelles à l'occasion d'une prise en charge sanitaire, médico-social ou des actions nécessaires à la coordination de ces prises en charge.
- Ces traitements ont pour base légale l'obligation légale (articles R. 1112-2 et R. 1112-7 du CSP) et reposent sur l'exception visée à l'article 9.2.h) du RGPD (traitements réalisés « aux fins de médecine préventive, *de diagnostics médicaux, de la de la prise en charge sanitaire ou sociale* (…) »).
- Les données administratives des patients et de leurs proches doivent être stockées de manière cloisonnée par rapport aux données de santé liées à la prise en charge des patients.
- Le NIR et l'INS constituent, par leur nature et leur usage, des identifiants qui doivent faire l'objet d'une protection renforcée, en particulier des habilitations d'accès spécifiques et une traçabilité renforcée. « *Ils pourraient faire l'objet d'un chiffrement spécifique au sein de la base administrative* », indique la CNIL.
- Les données structurées du DPI liées à la prise en charge doivent être cloisonnées (par rapport aux données administratives) et stockées sous forme pseudonymisée.

- Les données du DPI doivent faire l'objet d'un plan assurant une sauvegarde régulière des données, permettant leur restauration et la reprise d'activité en cas d'incident, étant précisé que la CNIL recommande que cette sauvegarde soit chiffrée.
- Les données doivent être conservées en base active pendant 20 ans à compter du dernier passage dans l'établissement et 10 ans à compter du décès de la personne (si celui-ci est intervenu moins de 10 ans après son dernier passage).
- Il est recommandé de formaliser une procédure concernant l'opportunité d'archiver les données en base intermédiaire.
- Sont précisées les conditions dans lesquelles (i) les membres de l'équipe de soins et (ii) le personnel ne relevant pas de l'équipe de soins peuvent avoir accès aux données.
- Des mesures de sécurité liées aux accédant sont également recommandées concernant les comptes utilisateurs et l'authentification multifacteur, la gestion des habilitations et la traçabilité des accès.

Qui peut contribuer ?

Ce document est soumis à la consultation publique jusqu'au 16 mai 2025.

Tous les établissements ainsi que leur délégué à la protection des données (DPO), leur conseil en matière de protection des données personnelles, leur médecin responsable de l'information médicale (DIM) et leurs responsables des systèmes d'information (DSI, RSSI) peuvent participer à cette consultation.

A suivre…

Alexandre Fievée

Alice Robert

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 ».

Enfin, en 2025, il fait son entrée dans le classement Chambers France, se positionnant en Band 3 dans le classement individuel Data Protection.

RENSEIGNEMENTS PRATIQUES

Prochaine session en 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