NEWSLETTER RGPD/DATA

NUMÉRO 55 ● 2023

SOMMAIRE

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

ACTUALITE

L'EMPLOYEUR NE PEUT INVOQUER LE RGPD POUR S'OPPOSER A UNE DEMANDE DE COMMUNICATION DE PIECES

Dans son arrêt du 1er juin 2023, la Cour de cassation s'est prononcée sur la possibilité, pour des salariés s'estimant discriminés, de demander en référé la communication des bulletins de paie de leurs collègues de travail.

Une trentaine de représentants du personnel, s'estimant victimes de discrimination en raison de leur activité syndicale, ont saisi, sur la base de l'article 145 du Code de procédure civile, le conseil de prud'hommes puis la cour d'appel, en référé, pour obtenir la communication, par leur employeur, de données permettant l'évaluation de leur situation au regard d'autres salariés.

La Cour d'appel a fait droit à leur demande et a ordonné la communication, sous astreinte, non seulement (i) des données d'identification des autres salariés embauchés concomitamment aux demandeurs, mais également (ii) de nombreuses autres données personnelles desdits salariés tels que : les diplômes, les bulletins de paie, les formations suivies, les dates de changement de qualification et classification.
Considérant une telle décision contraire au RGPD, l'employeur a formé un pourvoi en cassation invoquant l'argument selon lequel le traitement de données personnelles sollicité n'était (i) pas indispensable à l'exercice du droit à la preuve de la discrimination et (ii) pas proportionné au but poursuivi.

En effet, selon l'employeur, les bulletins de paie visés comportaient des données personnelles qui n'avaient pas de rapport avec le débat, comme : l'adresse postale, le numéro de sécurité sociale, le taux d'imposition, les absences, les congés ou encore la domiciliation bancaire.

Or, en l'espèce, la Cour d'appel se bornait à juger que ces éléments s'avéraient indispensables et les atteintes à la vie privée proportionnées, sans réelle motivation.
La question se posait donc de savoir si une telle motivation était suffisante ou si le juge n'était pas tenu de justifier de la communication ordonnée et ce, pour chaque type de donnée litigieuse.

La Cour de cassation rejette le pourvoi en énonçant que « *le droit à la protection des données à caractère personnel n'est pas un droit absolu et doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité* ».

Par suite, la Cour indique que « *le droit à la preuve peut justifier la production d'éléments portant atteinte à la vie personnelle à la condition que cette production soit indispensable à l'exercice de ce droit et que l'atteinte soit proportionnée au but poursuivi* ».
En l'espèce, la Cour d'appel relevait que les demandeurs n'avaient pas pu obtenir les éléments de comparaison demandés à leur employeur en dépit (i) de l'intervention du syndicat auprès de la direction, (ii) de la saisine du Défenseur des droits, (iii) de celle de l'inspecteur du travail ainsi (iv) que d'une mise en demeure. Le motif est donc jugé légitime.

Plus encore, ayant relevé que les éléments demandés étaient nécessaires aux demandeurs pour effectuer une comparaison utile, la cour juge qu'ils devaient disposer d'informations précises sur leurs collègues de travail et que *« la communication [des données] était indispensable et proportionnée au but poursuivi qui est la protection du droit à la preuve de salariés éventuellement victimes de discrimination et que la communication des bulletins de salaire avec les indications y figurant étaient indispensables et les atteintes à la vie personnelle proportionnées au but poursuivi* ».
En d'autres termes, le droit de la preuve peut justifier une immixtion profonde dans les données personnelles des autres salariés.

Source : ici

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

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

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

1. Les clauses contractuelles types

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

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

2. Les « *mesures supplémentaires* »

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

- Des mesures d'ordre organisationnel, composées d'un certain nombre de politiques et de procédures implémentées chez Meta Ireland et Meta US, par lesquelles Meta US s'obligeait notamment à :
    - Notifier à Meta Ireland tout réception d'une requête d'une autorité publique américaine, sauf prohibition de le faire en vertu de la loi ;
    - Soumettre un rapport détaillé à Meta Ireland quant aux fournitures de données sur la base des requêtes américaines.
- Des mesures d'ordre techniques, notamment par le chiffrement des données en transit
- Des mesures d'ordre légal, impliquant notamment l'obligation, pour Meta US, de former un recours contre les décisions émanant d'autorités américaines qu'elle estimait illégales, ou qui ne seraient pas nécessaires ou proportionnées dans une société démocratique.

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

3. Le décret présidentiel du 7 octobre 2022

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

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

4. La sanction

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

Source : ici

LE DROIT D'ACCES NE PERMET PAS D'OBTENIR L'IDENTITE DES PERSONNES AYANT CONSULTE LES DONNEES

Dans un arrêt du 22 juin 2023, la CJUE s'est prononcée sur les limites du droit d'accès en confirmant qu'on ne peut, en principe, pas d'obtenir l'identité des personnes ayant consulté ses données.

Le client d'une banque a appris que « *ses données avaient été consultées par des membres du personnel de la banque à plusieurs reprises* ».

Ayant des doutes sur la licéité de ces consultations, il a exercé son droit d'accès auprès de la banque afin que cette dernière lui communique « *(i) l'identité des personnes ayant consulté ses données, (ii) les dates exactes des consultations ainsi que (iii) les finalités du traitement desdites données* ».

Dans sa réponse, la banque a « *refusé de communiquer l'identité des salariés ayant procédé aux opérations de consultation au motif que ces informations constituaient des données à caractère personnel de ses salariés* ». Le client a saisi l'autorité de contrôle finlandaise afin qu'elle enjoigne à la banque de lui transmettre les informations sollicitées.

L'autorité de contrôle a rejeté la demande car une telle demande « *visait à permettre d'accéder aux fichiers journaux des salariés* » et que « *de tels fichiers constituent des données à caractère personnel relatives aux salariés* ».

Le client a fait appel de cette décision devant le tribunal administratif, qui a sursis à statuer pour poser à la CJUE une question préjudicielle. Le tribunal demande si la communication des « *fichiers journaux* », qui contiennent des informations sur l'identité des salariés, est couverte par l'article 15 du RGPD, dès lors que ces fichiers pourraient s'avérer nécessaires à la personne concernée pour apprécier la licéité du traitement.

Dans son arrêt, la CJUE a d'abord indiqué que l'article 15 du RGPD permettait d'obtenir la communication (i) des « *finalités du traitement* » et (ii) des « *dates des opérations de consultation* », ces dernières étant de nature à permettre à la personne concernée d'obtenir la confirmation que ses données font l'objet d'un traitement.

En ce qui concerne les « *fichiers journaux* », la CJUE a rappelé que « *la reproduction de documents […], qui contiennent, entre autres, les données à caractère personnel faisant l'objet d'un traitement qui peut s'avérer indispensable dans le cas où la contextualisation des données traitées est nécessaire pour en assurer l'intelligibilité* ». Ainsi, la transmission d'une copie des fichiers journaux *« peut s'avérer nécessaire* ».

Cependant, la CJUE a insisté sur le fait que l'exercice du droit d'accès « *ne devrait pas porter atteinte aux droits ou libertés d'autrui* », et qu'en cas de conflit entre l'exercice du droit d'accès et les droits et libertés d'autrui, il y a lieu de les mettre en balance et, dans la mesure du possible, « *de choisir des modalités qui ne portent pas atteinte aux droits ou aux libertés d'autrui* », sans pour autant « *aboutir à refuser toute communication d'informations* ». La CJUE a également rappelé (i) que les salariés du responsable du traitement *« ne sauraient être considérés comme étant des destinataires* » et (ii) que la personne concernée, si elle considère que les informations communiquées sont insuffisantes pour lui permettre de dissiper des doutes, a le droit de saisir l'autorité de contrôle d'une réclamation.

Compte tenu de ce qui précède, la CJUE considère que l'article 15 du RGPD doit être interprété en ce sens que :

- Les informations relatives à des opérations de consultation des données à caractère personnel d'une personne, portant sur les dates et les finalités de ces opérations, constituent des informations qu'une personne concernée a le droit d'obtenir ;

- En revanche, l'article 15 ne consacre pas un tel droit s'agissant des informations relatives à l'identité des salariés du responsable du traitement ayant procédé à ces opérations, sous son autorité et conformément à ses instructions, à moins que ces informations ne soient indispensables pour permettre à la personne concernée d'exercer effectivement sont droit d'accès.

Source : ici

COOKIES ET PUBLICITES CIBLEES SUR LE WEB : CRITEO CONDAMNEE A UNE AMENDE DE 40 MILLIONS D'EUROS.

La CNIL a prononcé une amende de 40 millions d'euros à l'encontre de la société de reciblage publicitaire Critéo pour de nombreux manquements au RGPD.

A la suite de plaintes déposées par les associations « *Privacy International* » et « *None Of Your Business* », à l'encontre de la société Critéo, la CNIL a diligenté une enquête en effectuant notamment plusieurs contrôles sur pièces et sur place.

La CNIL définit Critéo comme « *un intermédiaire entre des annonceurs et des éditeurs de sites web* » qui aide « *les annonceurs à troubler leur public cible avec des publicités plus pertinentes […] et les éditeurs à valoriser leurs espaces publicitaires* ». La société est plus précisément spécialisée dans le « *reciblage publicitaire* », qui consiste « *à suivre les habitudes de navigation des internautes pour leur afficher des publicités personnalisées, au moyen de cookies déposés dans les terminaux des utilisateurs* ».

Au terme de son enquête, la CNIL a retenu cinq manquements au RGPD à l'encontre de la société :

1. Manquement à l'obligation de démontrer que la personne a donné son consentement

Rappelant que « *dans les cas où le traitement repose sur le consentement, le responsable du traitement [doit être] en mesure de démontrer que la personne concernée a donné son consentement* », l'autorité de contrôle a constaté que la société n'était pas en mesure de démontrer l'existence dudit consentement.

D'ailleurs, selon la CNIL, le fait que « *la collecte du consentement des internautes […] revienne aux partenaires n'exonère pas la société de son obligation* ».

Compte tenu de cette impossibilité de démontrer l'existence d'un consentement valide, la CNIL a considéré que la société a violé l'article 7 du RGPD.

2. Manquement à l'obligation d'information et de transparence

La CNIL a considéré que *« l'information fournie par la société aux personnes concernées n'était pas complète* » et que la base juridique applicable « *manqu[ait] de clarté* ».

Plus précisément, elle considérait que les formulations employées par Critéo créaient une incertitude (i) « *quant à la base juridique du traitement* » car l'internaute ne pouvait pas comprendre que le traitement reposait sur son consentement et (ii) sur la finalité, puisque la formulation employée utilisait « *des termes vagues et larges* ».

Selon la CNIL, « *en ne délivrant pas aux personnes concernées l'intégralité des informations prévues en ayant recours à des termes insuffisamment clairs et précis et en présentant une base juridique […] erronée, la société a manqué à ses obligations de transparence et d'information prévues aux articles 12 et 13 du RGPD* ».

3. Manquement au respect du droit d'accès

Dans le cadre des investigations menées par la CNIL, Critéo a fourni à la délégation trois exemples de réponses adressées à des personnes concernées ayant formulé des demandes d'accès.

Après analyse desdites réponses, la CNIL a considéré que la société « *ne répondait que partiellement aux demandes* » et que la réponse « *n'était pas intelligible* ».

Effectivement, l'autorité de contrôle considère que les réponses apportées (i) ne communiquaient pas « *l'intégralité des données à caractère personnel des personnes exerçant leur droit d'accès* » et (ii) ne mettaient pas « *d'office à leur disposition une documentation leur permettant de comprendre les données qui leur étaient communiquées* ».

Compte tenu de ce qui précède, la CNIL a considéré que la société avait manqué à ses obligations au titre des articles 12 et 15 du RGPD.

4. Manquement au respect du droit de retrait du consentement et de l'effacement des données

La CNIL a constaté que « *les personnes concernées qui souhaitaient retirer leur consentement […] ou qui exerçaient leur droit à l'effacement pouvaient le faire en cliquant sur un bouton […] accessible dans la politique de confidentialité* ».

Cependant, lorsqu'une telle action était effectuée par la personne concernée, Critéo se limitait « *à interrompre l'affichage des publicités ciblées dans le terminal de la personne […] sans procéder à un effacement* » des données.
Constatant que la société, bien qu'étant « *en capacité de procéder à un effacement effectif des données* », n'a pas réalisé ledit effacement, la CNIL a considéré qu'elle manqué à ses obligations au titre des articles 7 et 17 du RGPD.

5. Manquement à l'obligation de prévoir un accord entre responsables conjoints du traitement

Rappelant l'obligation, pour les responsables conjoints du traitement, de conclure un accord, la CNIL a considéré que l'accord conclu entre Critéo et les responsables du traitement conjoints n'était pas conforme au RGPD.

En effet, l'autorité de contrôle a remarqué que « *l'accord conclu par la société avec ses partenaires ne précisait pas certaines obligations […] telles que l'exercice par les personnes concernées de leurs droits, l'obligation de notification d'une violation de données à l'autorité de contrôle et aux personnes concernées ou bien, le cas échéant, la réalisation d'une étude d'impact* ».

La CNIL a donc considéré que la société avait manqué à son obligation au titre de l'article 26 du RGPD.

Compte tenu de tout ce qui précède, la CNIL a infligé à Critéo une amende de 40 millions d'euros.

Source : ici

LA SANCTION CNIL QUE LA SOCIETE DE VOYANCE AURAIT PU PREDIRE

Le 8 juin 2023, la CNIL a prononcé une sanction à l'égard de KG COM, en raison de multiples manquements, dont : un défaut de notification d'une violation de données, une atteinte au principe de minimisation et un traitement de données sensibles sans consentement.

Alertée par un article de presse du 1er octobre 2020, la CNIL, qui a pris connaissance d'une ayant affecté des données personnelles traitées par une société de voyance, KG COM, a diligenté un contrôle sur pièces, puis un contrôle en ligne, et enfin un contrôle sur place.

1. Principe de minimisation

La société enregistrait systématiquement les appels téléphoniques passés avec ses prospects, ainsi qu'entre ses voyants et ses clients, à des fins de contrôle qualité, de preuve de la souscription du contrat et « *dans la perspective de réquisitions judiciaires* ».

Pour la CNIL :

- l'enregistrement systématique de l'intégralité des conversations téléphoniques n'étaient pas justifié par la finalité de contrôle qualité, qui aurait pu être atteinte avec des enregistrements ponctuels et aléatoires ;
- l'enregistrement de la conversation ne peut servir de preuve de la souscription d'un contrat que dans l'hypothèse où il n'existe pas d'autres moyens moins intrusifs, ce qui n'étais pas le cas en l'espèce, l'article L221-16 du Code de la consommation imposant, au contraire, à la société, la conclusion d'un contrat signé sur un support durable
- « *s'il est nécessaire que les responsables du traitement fassent droit aux réquisitions judiciaires qu'ils reçoivent concernant les données qu'ils traitent pour leurs propres besoins, ils n'ont en revanche pas à organiser, à l'avance, la collecte de données à caractère personnel dans la perspective de répondre à une potentielle réquisition judiciaire* ».

2. Principe de conservation limitée

Les contrôles ont également mis en lumièreun manquement à l'obligation de conservation limitée. En effet, alors que la société affirmait conserver les données des clients 3 ans en base active à compter de la fin de la relation commerciale, la CNIL a toutefois constaté que les données de certains clients étaient conservées depuis plus de 5 ans en base active après la dernière consultation.

3. Défaut de base légale

La CNIL a appris que les données de cartes bancaires des clients étaient conservées au-delà du temps nécessaire à la transaction, afin que les clients n'aient pas à ressaisir leur numéro de carte lors de leurs achats ultérieurs. Pour la CNIL, ce traitement ne peut pas reposer sur la base légale de l'exécution contractuelle et nécessite le consentement des clients, ce qui n'était pas le cas en l'espèce.

4. Traitement de données sensibles sans consentement

Lors des consultations entre clients et voyants, ces derniers collectent des données relatives à la santé et l'orientation sexuelle des clients, sans que l'accord des clients ne soit, toutefois, recueilli. En effet, pour la CNIL, la simple expression de volonté de recevoir une prestation de voyance et de livrer spontanément des informations sensibles ne constitue pas un consentement univoque, ni, en l'absence d'information dédiée, éclairé, à voir lesdites informations être traitées. La CNIL en a conclu que le traitement de données sensibles, par la société, n'était pas conforme au RGPD.

5. Principe de transparence

La CNIL a relevé que les informations relatives aux traitements étaient accessibles depuis la page d'accueil du site internet de la société, mais n'étaient pas visibles dans le formulaire de création de compte dudit site. Par ailleurs, ces informations se trouvaient dans un document intitulé « CGV » comprenant à la fois des informations sur les conditions de vente, sur les conditions d'utilisation du site web, et sur les traitements de données à caractère personnel. Certaines informations, telles que la durée de conservation, le droit à la portabilité et le droit d'introduire une réclamation auprès de l'autorité de contrôle, faisaient défaut.

6. Obligation de sécurité

La CNIL a relevé de multiples manquements en matière de sécurité, notamment l'usage du protocole « http » au lieu de « https », ainsi que des mots de passes insuffisamment sécurisés.

En conséquence de l'ensemble de ces manquements, la CNIL a condamné la société KG COM au paiement d'une amende administrative de 150.000 €.

Source : ici

LES ETATS-UNIS, DE NOUVEAU RECONNUS PAYS « ADEQUAT »

Par une décision du 10 juillet 2023, la Commission Européenne a reconnu, pour la troisième fois, les Etats-Unis comme garantissant un niveau de protection adéquat pour le transfert de données à caractère personnel.

Après avoir reconnu les Etats-Unis, une première fois, comme un pays « *adéquat* » dans sa première décision d'adéquation du 26 juillet 2000, dite « *Safe Harbor* », (invalidé par la CJUE dans son arrêt du 6 octobre 2015), puis une deuxième fois dans sa deuxième décision d'adéquation du 12 juillet 2016, dite « *Privacy Shield* », (invalidé par la CJUE dans son arrêt du 16 juillet 2020), la Commission européenne a reconnu une troisième fois les Etats-Unis comme un pays « *adéquat* ».

Par une décision d'exécution du 10 juillet 2023, la Commission Européenne a en effet considéré que « *les Etats-Unis garantissent un niveau de protection adéquat pour les données à caractère personnel transférées de l'Union vers des organisations des Etats-Unis qui figurent sur la " Data Privacy Framework List " ».*

Cette décision d'exécution fait suite à un long processus législatif annoncé par la Commission dès le 13 décembre 2022.

Le système de transfert sera similaire à celui utilisé par le « *Safe Harbor* » : seuls pourront s'effectuer librement, sans encadrement spécifique, les transferts de données personnelles depuis l'Union européenne à destination d'organismes situés aux Etats-Unis qui figurent sur une liste (la Data Privacy Framework List) publiée sur le site : https://www.dataprivacyframework.gov/s/

A ce jour, plus de 2500 organismes américains, et en premier lieu les plus connus tels que Meta, Google, Microsoft ou Amazon, figurent déjà sur la liste. Cela signifie donc (i) que ces entités se sont engagées à respecter les principes posés par le « *Data Privacy Framework* », et (ii) que les transferts de données personnelles vers ces entités sont désormais possibles sans qu'il soit nécessaire d'utiliser d'autres garanties (garanties appropriées) et autres mesures complémentaires.

Des recours contre cette décision d'adéquation ont déjà été annoncés : affaire à suivre…

Source : ici

DOCTRINE

RGPD

Obtenir sa copie d'examen via le droit d'accès ?

Comme chaque mois, Alexandre Fievée tente d'apporter des réponses aux questions que tout le monde se pose en matière de protection des données personnelles, en s'appuyant sur les décisions rendues par les autorités nationales de contrôle au niveau européen et les juridictions nationales et européennes. Ce mois-ci, il se penche sur la problématique de l'efficacité d'une demande de droit d'accès exercée par un étudiant aux fins d'obtenir la communication d'une copie de sa copie d'examen.

L'exercice du droit d'accès, visé à l'article 15 du RGPD, permet à toute personne de savoir si des données la concernant sont traitées par un organisme déterminé puis d'en obtenir, si elle le souhaite, une copie dans un format compréhensible. Cette démarche permet notamment de contrôler la licéité du traitement, mais aussi l'exactitude des données et, au besoin, de les faire rectifier ou effacer. Telle est la finalité intrinsèque du droit d'accès, ainsi exprimée au considérant 63 du RGPD. Mais, en réalité, le droit d'accès ne connaît pas de limite sur ce terrain-là.

En application d'une « *jurisprudence* » constante de la CNIL (mais aussi du CEPD), l'organisme ne peut, pour écarter une demande de droit d'accès, invoquer l'abus de droit au motif que cette demande poursuivrait une autre finalité que celle de vérifier la licéité d'un traitement. En d'autres termes, le fait que le droit d'accès permette d'obtenir des informations pour un autre motif que celui visé au considérant 63 est indifférent, même si cela permet à la personne concernée d'obtenir des données qu'elle n'aurait pas pu obtenir par une autre voie.

Ceci ne veut pas dire pour autant que le droit d'accès ne connaît pas de limites. Elles sont énumérées au paragraphe 4 de l'article 15 du RGPD : si l'organisme sollicité doit permettre un accès aux données à la personne concernée qui en fait la demande, cela ne peut concerner que les données dont la communication ne porte pas une atteinte disproportionnée aux droits d'autrui, tels que le secret des affaires, la propriété intellectuelle, le droit à la vie privée, ou encore le secret des correspondances. Un étudiant qui se voit opposer un refus à une demande de communication d'une copie de sa copie d'examen peut-il, en application du droit d'accès, exiger une telle communication ? Tel est l'objet de cette affaire.

L'affaire[1]

Après avoir échoué à un test de langue, la requérante a réclamé la remise de la copie de sa copie d'examen. La défenderesse lui a alors proposé de venir consulter le document dans ses locaux, ce que la requérante a refusé. Cette dernière a saisi le tribunal de Francfort, considérant avoir droit à la communication de sa copie d'examen en application de l'article 15, paragraphe 3 du RGPD. La juridiction allemande a estimé, au contraire, que la requérante ne pouvait, en application, de ce texte, exiger sa copie d'examen, même si elle reconnaît que la copie en question contient des données personnelles : « *Certes (...) les réponses de la demanderesse aux questions d'examen et les remarques des examinateurs constituent toutes des données à caractère personnel (...). Mais cela ne s'applique toutefois pas aux questions d'examen en tant que telles.* »

Par ailleurs, et surtout, le tribunal va considérer que la défenderesse pouvait, à juste titre, opposer un intérêt au secret, conformément aux termes de l'article 15, paragraphe 4 du RGPD : « *Il ressort en particulier du manuel pour le développement et la réalisation de tests linguistiques (...) qu'il s'agit d'une procédure scientifiquement fondée et couteuse, à laquelle participent un grand nombre de personnes, ce qui implique des dépenses considérables. Les questions d'examen constituent donc, d'un point de vue juridique, des secrets d'affaires (...) et des œuvres linguistiques protégées par le droit d'auteur (...)* ». La juridiction allemande a donc, dans ce cas d'espèce,

privilégié les intérêts de la défenderesse sur ceux de la personne concernée, dès lors que « *la mise à disposition d'une copie de la copie d'examen s'accompagne nécessairement d'une violation des intérêts en matière de confidentialité en ce qui concerne les questions d'examen* ». Un autre élément a emporté la conviction du juge : le fait que le droit d'accès n'était pas totalement entravé, puisque la défenderesse offrait la possibilité à la personne concernée de consulter la copie d'examen dans ses locaux.

Quelles recommandations ?

Il résulte de ce qui précède que, sauf à démontrer que l'examen repose sur une procédure scientifique et, le cas échéant, sur une procédure « *protégée* » par un droit privatif, il sera difficile pour une école ou une université de s'opposer légitimement à une demande de droit d'accès émanant d'un étudiant manifestant son souhait d'obtenir une copie de sa copie d'examen. Il existerait toutefois une parade, qui repose sur un des fondamentaux du droit d'accès : ce droit porte uniquement sur les données personnelles et non sur des documents. En d'autres termes, si l'organisme doit fournir une copie des données personnelles concernant la personne qui en fait la demande, il n'a pas à communiquer les documents contenant les données. Il pourrait ainsi se contenter de fournir les seules informations se rattachant à l'étudiant concerné : note, appréciations, annotations et éventuellement (à discuter) les réponses aux questions, à l'exclusion bien entendu des questios de l'examen en tant que telles.

Alexandre FIEVEE
Avocat associé
DERRIENNIC Associés

Notes

(1) AG Frankfurt Juge Unique, 14 mars 2023.

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

ÉCHOS DE LA PRATIQUE

NUMÉRIQUE

625

3 QUESTIONS

CJUE : la question de la révocation du DPO et la notion de conflit d'intérêts

Alexandre Fievée,
avocat associé, Derriennic Associés
Alice Robert,
avocat of Counsel, Derriennic Associés

1 Dans quel contexte, la question de la révocation du DPO est-elle revenue sur le devant de la scène judiciaire ?

Dans deux arrêts du 9 février dernier, la CJUE a donné des indications précieuses concernant la question de la révocation du DPO et la notion de conflit d'intérêts.

C'est à l'occasion de deux litiges allemands que la CJUE a été saisie de questions préjudicielles sur ces deux sujets. Dans une première affaire, une société avait relevé de ses fonctions son DPO salarié au motif qu'il existait un risque de conflit d'intérêts, le DPO exerçant en même temps les fonctions de président du comité d'entreprise. Dans une seconde affaire, une commune avait relevé de ses fonctions son DPO salarié au motif qu'il existait un conflit d'intérêts entre ses activités de DPO et ses autres activités professionnelles. Les DPO concernés ont saisi les juridictions allemandes et se sont appuyés sur une réglementation nationale prévoyant qu'un DPO salarié ne peut être révoqué de ses fonctions que pour un « motif grave ».

2 Quels sont les cas possibles de révocation du DPO ?

Pour mémoire, l'article 38, § 3 du RGPD prévoit que : « *le délégué à la protection des données ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions* ».

Pour autant, la CJUE a considéré que le RGPD « *ne s'oppose pas à une réglementation nationale prévoyant qu'un responsable du traitement ou un sous-traitant ne peut révoquer un [DPO] qui est membre de son personnel que pour un motif grave, même si la révocation n'est pas liée à l'exercice des missions de ce [DPO]* ». La CJUE a cependant émis une réserve, en considérant « *qu'une telle réglementation ne [doit pas compromettre] la réalisation des objectifs de ce règlement* ». Tel serait le cas, par exemple, si la réglementation nationale empêchait toute révocation d'un DPO qui ne posséderait plus les qualités professionnelles requises pour exercer ses missions (conformément à l'article 37, § 5 du RGPD), ou qui ne s'acquitterait pas de celles-ci conformément au RGPD. Cette solution va dans le même sens qu'un précédent arrêt de la Cour (*CJUE, 22 juin 2022, aff. C-534/20, Leistritz : Europe 2022, comm. 266, obs. F. Gazin*), dans lequel la CJUE avait considéré qu'une réglementation nationale ne peut empêcher la révocation du DPO dans l'hypothèse où il ne serait plus en mesure d'exercer ses tâches en toute indépendance en raison de l'existence d'un conflit d'intérêts.

Suite page 6

En mouvement

Casalonga a le plaisir d'annoncer la nomination de ***Pascaline Vincent*** en qualité d'associée.

Avocate depuis 2008, Pascaline Vincent a rejoint le Cabinet Casalonga en 2011 et a aujourd'hui plus de 15 ans d'expérience dans la propriété intellectuelle, les contrats et l'innovation.

Elle intervient auprès de sociétés françaises et internationales dans tous les domaines de la propriété intellectuelle (brevets, marques, dessins et modèles, droit d'auteur) tant en conseil qu'en contentieux. Pascaline accompagne les clients dans leur stratégie globale de création et d'innovation, dans la rédaction et la négociation de leurs contrats et dans la défense de leurs droits devant les offices et les tribunaux. Elle a également développé une expertise dans les litiges relatifs aux brevets essentiels et dans le fonctionnement de la JUB.

3 Comment apprécier une situation de conflit d'intérêts du DPO ?

Pour rappel, l'article 38, § 6 du RGPD précise que « *Le délégué à la protection des données peut exécuter d'autres missions et tâches. Le responsable du traitement ou le sous-traitant veillent à ce que ces missions et tâches n'entraînent pas de conflit d'intérêts* ». Pour la CJUE, cela signifie que le DPO ne saurait se voir confier l'exécution de missions ou tâches qui seraient susceptibles de nuire à l'exercice de ses fonctions qu'il exerce en tant que DPO. Un conflit d'intérêts est ainsi susceptible d'exister, selon la CJUE, « *lorsqu'un DPO se voit confier d'autres missions ou tâches qui le conduiraient à déterminer les finalités et les moyens du traitement de données à caractère personnel auprès du responsable de traitement ou de son sous-traitant* ». Cette situation doit cependant être déterminée par le juge national, « *au cas par cas* », « *sur la base d'une appréciation de l'ensemble des circonstances pertinentes, notamment de la structure organisationnelle responsable de traitement ou de son sous-traitant et à la lumière de l'ensemble de la réglementation applicable, y compris d'éventuelles règles internes de ces derniers* ».

Cette jurisprudence s'inscrit dans la lignée de la « doctrine » du CEPD et de la CNIL qui considèrent que le DPO, qui doit être indépendant, ne peut occuper un poste qui le conduirait à déterminer les finalités et les moyens d'un fichier. En d'autres termes, il ne peut pas être « juge et partie ». Si la CNIL n'a jamais, à notre connaissance, sanctionné un organisme pour un motif de « conflit d'intérêts », d'autres autorités de contrôle en Europe l'ont fait. Tel est le cas notamment de l'autorité luxembourgeoise (CNPD) qui a retenu un tel grief concernant un DPO qui exerçait les fonctions de directeur de la conformité (*CNPD (Luxembourg), délib. n° 37FR/2021, 13 oct. 2021*), mais aussi de l'autorité allemande (BBDI) concernant un DPO qui occupait le poste de directeur général d'une filiale, société de service du groupe (*BBDI (Allemagne), communiqué, 20 sept. 2022*).

Focus

626

L'AMF publie sa cartographie 2023 des marchés et des risques

Le 6 juillet 2023, l'Autorité des marchés financiers (AMF) a publié sa traditionnelle cartographie des marchés et des risques, qui, cette année se concentre essentiellement sur l'installation durable de l'inflation, l'accélération de la normalisation des politiques monétaires, le risque de correction sur les marchés financiers et la dégradation des conditions de financement.

En 2022, les marchés ont connu une correction sensible à l'image du CAC 40 (dividendes réinvestis) qui a baissé de 6,7 %. L'effondrement du TerraLuna, en mai 2022, ou encore la faillite de la plateforme FTX, en novembre 2022, ont également provoqué une forte baisse du marché des crypto-actifs. Toutefois, depuis début 2023, nous avons assisté à un net rebond du CAC 40, qui a atteint des niveaux historiques limitant la correction connue jusqu'à présent. Dans un contexte d'incertitude, le risque de baisse des prix d'actifs demeure substantiel. En termes de stabilité financière, les acteurs des marchés financiers doivent s'adapter au nouvel environnement de taux qui entraîne une raréfaction relative de la liquidité et pourrait se traduire par une hausse des risques de crédit.

Le risque de correction des marchés demeure très élevé et dépend grandement de la capacité des acteurs à s'adapter à ce nouvel environnement de taux. - Cette édition de la cartographie met notamment en lumière des évènements récents qui illustrent la matérialisation des risques liés aux vulnérabilités de certains acteurs dans un environnement de taux élevés. Au Royaume-Uni, le recours au levier des fonds de pension à prestations définies a entraîné des ventes massives sur les marchés d'obligations d'État et une intervention de la Banque d'Angleterre afin de limiter le risque systémique. Au premier trimestre 2023, des retraits rapides de dépôts de plusieurs banques régionales américaines et les faillites qui ont suivi illustrent également le risque de liquidité en lien avec la question de la valorisation des actifs.

La hausse des taux augmente également le risque de crédit, dégrade la soutenabilité de la dette et affecte la capacité de refinancement. - La conjoncture de taux exerce un effet direct sur le coût du crédit et peut aussi rendre plus difficile le refinancement du stock de dette. Sur le segment des obligations d'entreprises, par exemple, les conditions de liquidité se sont nettement dégradées et la volatilité a fortement augmenté depuis le printemps 2022. Cette pression sur les coûts de financement pourrait entraîner une augmentation des défauts, notamment parmi les entreprises classées en catégorie spéculative par les agences de notation.

À ce stade, l'AMF a observé une baisse des encours des fonds français en 2022, liée essentiellement à un effet de valorisation. Les fonds monétaires ont bénéficié de la hausse de taux avec un impact positif sur leurs rendements à partir du dernier trimestre 2022. L'AMF demeure vigilante quant aux fonds d'investissement exposés au secteur de l'immobilier commercial, à la suite d'une forte contraction de volumes de transactions et des prix. Le secteur du capital investissement montre également des signes de baisse d'activité marquée par une diminution des investissements et des opérations de désinvestissement. Cela pose la question des conditions de refinancement de ces acteurs dans un contexte de taux plus élevé.

Le contexte de hausse des taux favorise les comptes à termes et les livrets réglementés. - Après s'être contractée au second semestre 2022, l'activité des investisseurs particuliers en bourse augmente légèrement début 2023. L'AMF constate également une réallocation de l'épargne en faveur des livrets réglementés et, fait nouveau, des comptes à termes. Dans une bien moindre mesure, l'activité des investisseurs particuliers en bourse augmente légèrement en 2023 après s'être contractée au second semestre 2022. L'appétit pour le risque apparaît encore modéré pour les particuliers.

Enfin, cette cartographie fait le constat que certains risques structurels demeurent élevés. Le risque de cyber-attaques s'est accru dans un contexte de tensions géopolitiques fortes dans plusieurs régions du monde (*AMF, communiqué, 6 juill. 2023*).

PANORAMA EUROPÉEN

PANORAMA DE QUELQUES DECISIONS RENDUES PAR DES AUTORITÉS NATIONALES DE CONTRÔLE

L'employeur n'a pas à informer le personnel du motif du licenciement d'autres salariés

APD (Belgique), 1er juin 2023

L'autorité de contrôle belge a prononcé un avertissement à l'encontre d'un employeur qui a indiqué au personnel que des salariées avaient été licenciées « pour faute grave ».

Deux salariées d'un établissement prenant en charge des enfants ont été licenciées pour faute grave.

L'employeur a transmis un courriel au reste du personnel mentionnant que les deux femmes avaient été « licenciées pour faute grave ».

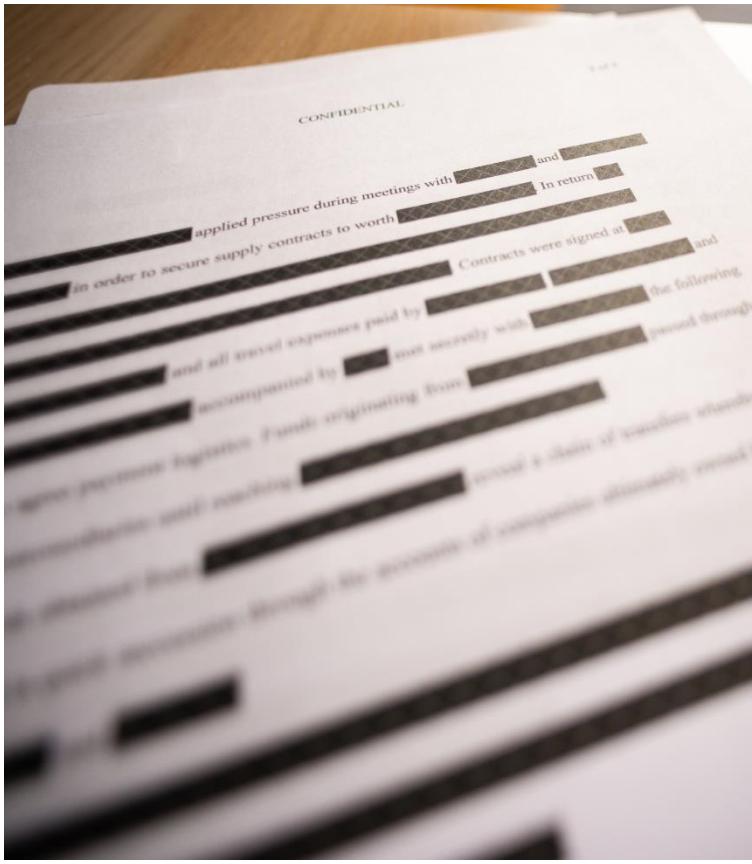
Considérant que la précision sur la nature de leur licenciement (i) n'était pas nécessaire et (ii) pouvait donner l'impression qu'elles avaient commis une faute grave par rapport aux enfants pris en charge, elles ont déposé une plainte auprès de l'autorité de contrôle belge.

Après avoir rappelé le principe de minimisation, cette dernière a considéré qu'il « n'est pas nécessaire de préciser la nature du licenciement afin d'informer les collaborateurs […] la seule mention du départ étant suffisante ».

Compte tenu de ce qui précède, l'autorité de contrôle a prononcé un avertissement à l'encontre du responsable du traitement en lui demandant « de respecter à l'avenir […] l'article 5.1.c) du RGPD ».

Source : ici

Autorité de protection des données
Gegevensbeschermingsautoriteit



La réponse d'un médecin à un commentaire sur internet ne doit pas révéler de données personnelles

LDI NRW (Allemagne), 2022

Une autorité de contrôle allemande a sanctionné un médecin qui, en répondant à un commentaire négatif sur internet, a dévoilé les données personnelles d'un de ses patients.

Un patient, visiblement mécontent de sa consultation avec un médecin, a publié un commentaire négatif à propos de ce dernier sur internet.

Estimant ce commentaire injustifié, le médecin a répondu en révélant des informations sur (i) la visite médicale, (ii) le diagnostic et (iii) le résultat du traitement du patient.

Ce dernier a déposé une plainte auprès de l'autorité de contrôle allemande qui a précisé que si, d'un côté, les patients peuvent user de leur liberté d'expression pour évaluer des médecins en ligne (à condition de respecter les limites imposées par le droit pénal et civil), les médecins peuvent, de l'autre côté, répondre aux commentaires à condition, toutefois, de ne pas enfreindre la législation sur la protection des données personnelles ou le secret médical.

Constatant, en l'espèce, que les données divulguées par le médecin étaient des données de santé, l'autorité de contrôle allemande a considéré que le médecin avait enfreint l'article 9 du RGPD et a infligé à ce dernier une amende dont le montant n'a pas été dévoilé.

Source : ici

La restitution d'un dossier par l'avocat ne peut pas passer par le droit d'accès

APD (Belgique), 12 juin 2023

L'autorité de contrôle belge s'est déclarée incompétente pour ordonner la restitution d'un dossier de procédure judiciaire par un avocat à la plaignante.

A la suite du décès de son avocat, le dossier d'une cliente a été transféré à un nouvel avocat sans son consentement.

Ne souhaitant pas confier son dossier à ce nouvel avocat, la cliente a sollicité sa restitution.

Après avoir effectué de multiples demandes au nouvel avocat, restées sans réponse, la cliente a saisi le bâtonnier qui a considéré qu'il ne lui appartenait pas « de faire quelque injonction au défendeur ».

La cliente a déposé une plainte auprès de l'autorité de contrôle belge.

Après avoir analysé la demande, l'autorité de contrôle belge a décidé de classer la plainte sans suite au motif que :

- *« aucune demande basée sur le RGPD n'a été formulée par la plaignante* », et donc « aucun manquement au RGPD ne peut être constaté », la plaignante n'ayant identifié ni suggéré aucun grief tiré d'un éventuel manquement au RGPD ;

- « *c'est sur le plan du respect des règles déontologiques et professionnelles de l'avocat que se place la plaignante pour obtenir la restitution et la communication de son dossier* », étant donné que l'autorité de contrôle considère n'avoir « aucune compétence pour ordonner la restitution d'un dossier de procédure *judiciaire par un avocat à la plaignante ».*

Autorité de protection des données
Gegevensbeschermingsautoriteit

Souhaitant faire preuve de pédagogie, l'autorité de contrôle a ajouté que si « *le dossier de procédure judiciaire réclamé par la plaignante contient, selon toute vraisemblance, des données à caractère personnel la concernant au regard desquelles elle peut exercer le droit d'accès que lui reconnait l'article 15 du RGPD »,* une telle demande n'emporterait toutefois pas nécessairement *« la restitution du dossier judiciaire sollicité dans son intégralité mais bien uniquement la communication des données personnelles relatives à la plaignante conformément […] à l'article 15 du RGPD ».*

L'autorité de contrôle a enfin considéré que « *même si on devait interpréter la plainte comme une demande fondée sur l'article 15 du RGPD, [l'autorité de contrôle] n'en classerait pas moins la plainte sans suite […] en ce que la plainte s'inscrirait dans le cadre d'un conflit plus large de restitution d'un dossier* ».

Source : ici

Elle découvre les condamnations pénales de son conjoint sur un site internet et le quitte. Il demande réparation auprès du site internet

Cass. Civ. (Italie), 7 mars 2023

La Cour de cassation italienne a effectué une mise en balance entre le droit à l'oubli et l'intérêt légitime du public à la connaissance d'un fait en prenant position pour ce dernier.

Dix-huit ans après avoir purgé sa peine pénale pour des délits liés à la drogue, un homme a refait sa vie.

A l'occasion d'une recherche sur internet, sa fiancée est tombée sur un vieil article de presse relatant l'arrestation de l'homme. Découvrant ses antécédents judiciaires, la fiancée a mis fin à cette relation et l'homme est tombé en dépression.

L'homme a exercé son droit à l'effacement auprès de l'agence de presse éditrice du site web et a sollicité une réparation de son préjudice.

L'agence de presse a fait droit à la demande d'effacement, mais a refusé de réparer le préjudice.

Les juges du fond ont rejeté la demande de l'homme au considérant que « le droit à l'oubli n'entraîne pas automatiquement l'obligation pour un journal de supprimer ou désindexer un article ».

L'homme a formé un pourvoi devant la Cour de cassation.

La Cour a considéré qu' « en matière de traitement des données à caractère personnel et de droit à l'oubli […] l'éditeur d'un site web n'est pas tenu d'effectuer la suppression, la désindexation ou la mise à jour d'un article de presse licitement publié, même s'il porte sur des faits remontants dans le temps, en l'absence d'une demande de la personne concernée ».

Bien au contraire, la Cour a considéré qu' « *imposer aux éditeurs de sites internet un tri périodique des informations qui ont été légitimement publiées à l'époque leur imposerait une charge insupportable et lourde de conséquences pour la liberté d'information* ».

Compte tenu de tout ce qui précède, la Cour de cassation a rejeté la requête de l'homme et l'a condamné aux dépens.

Source : ici

ACTUALITÉS DU CABINET

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

OBJECTIFS

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

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

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

CONTENU DE LA FORMATION

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

COÛT

3000€ HT/personne

INTERVENANT

Alexandre FIEVEE
Avocat Associé
01.47.03.14.94
afievee@derriennic.com

CLASSEMENTS

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

RENSEIGNEMENTS PRATIQUES

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