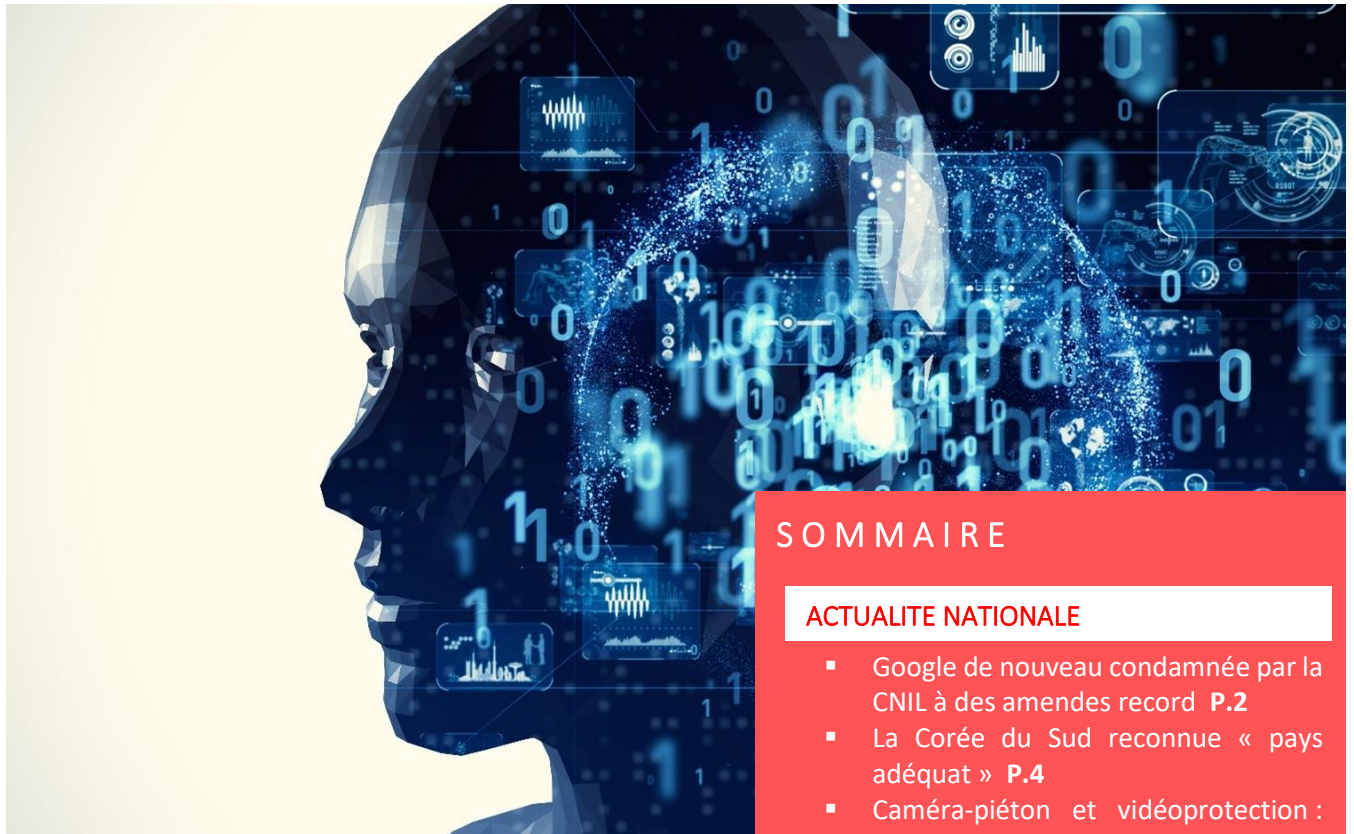




NEWSLETTER RGPD

NUMÉRO 39 • JANVIER 2022



ACTUALITE DU CABINET

FORMATION A LA PREPARATION A LA CERTIFICATION « DPO ».

Le cabinet organise régulièrement des programmes de formation visant à la préparation des apprenants à l'examen de certification « DPO ».



Retrouvez notre programme à la fin de notre newsletter **P.18**

SOMMAIRE

ACTUALITE NATIONALE

- Google de nouveau condamnée par la CNIL à des amendes record **P.2**
- La Corée du Sud reconnue « pays adéquat » **P.4**
- Caméra-piéton et vidéoprotection : une commune mise en demeure par la CNIL **P.5**
- SLIMPAY condamnée par la CNIL pour violation de données **P.6**
- Publication d'un guide RGPD à l'attention des développeurs **P.8**
- Précisions de la CEDH sur la portée du droit à l'oubli **P.9**
- Le Parlement européen rappelé à l'ordre par le CEPD en raison d'un transfert de données vers les Etats-Unis **P.12**

VU DANS LA PRESSE

- L'envoi d'un courriel à un destinataire erroné doit-il être notifié ? **P.13**

ACTUALITE EUROPEENNE

- Panorama de quelques décisions rendues par des autorités nationales de contrôle **P.16**

GOOGLE DE NOUVEAU CONDAMNÉE PAR LA CNIL A DES AMENDES RECORD

La CNIL a condamné Google à deux amendes record (90 millions d'euros pour GOOGLE LLC et 60 millions d'euros pour GOOGLE IRELAND LIMITED), en raison d'un processus de recueil du consentement à l'utilisation des cookies non conforme au cadre réglementaire applicable.


Pour rappel, à la suite d'un contrôle diligenté en 2020, la CNIL avait condamné GOOGLE LLC et GOOGLE IRELAND LIMITED à deux amendes d'un montant cumulé de 100 millions d'euros pour dépôt de cookies sans recueil préalable du consentement, défaut d'information quant à l'utilisation des cookies et défaillance partielle du mécanisme d'opposition aux cookies (décision ayant fait l'objet d'un [article sur notre site](#)).

Suite à ce contrôle et à cette sanction, la CNIL avait considéré, par une délibération du 30 avril 2021, que GOOGLE LLC et GOOGLE IRELAND avaient satisfait à l'injonction de mettre en conformité le site « google.fr » aux règles applicables en matière de cookies.

Parallèlement, au mois de mars, avril, juin et juillet 2021, la CNIL a été saisie de plusieurs plaintes dénonçant les modalités de refus des cookies sur les sites « google.fr » et « youtube.com », ce qui a entraîné un contrôle en ligne sur ces deux sites.

Ce contrôle a révélé que le bandeau affiché sur ces deux sites contenait bien un bouton permettant d'accepter immédiatement les cookies, mais qu'« aucun moyen analogue » n'était proposé à l'utilisateur pour pouvoir refuser, aussi facilement, le dépôt de ces cookies. Cinq actions étaient en effet nécessaires à l'utilisateur pour pouvoir refuser les cookies. La CNIL y a vu une méconnaissance des « exigences légale de liberté du consentement ».

En défense, GOOGLE LLC et GOOGLE IRELAND LIMITED ont soutenu que la CNIL ne pouvait se prononcer une nouvelle fois sur les mêmes faits que ceux concernés par la délibération de 2020, sans violer le principe « non bis in idem ». La CNIL a indiqué que les faits étaient différents, la procédure d'espèce portant sur les modalités de refus des cookies, et non sur l'information liée aux cookies.



Les deux sociétés ont également estimé que la CNIL n'était pas compétente, en vertu du mécanisme de « *guichet unique* » prévu par le RGPD. La CNIL a répondu que ce mécanisme n'avait pas vocation à s'appliquer en l'espèce, dans la mesure où les cookies relèvent de la directive « ePrivacy », transposée à l'article 82 de la loi « Informatique et Libertés » du 6 janvier 1978, et non du RGPD. La CNIL, afin de justifier sa compétence territoriale, a estimé que le recours aux cookies avait lieu dans le « *cadre des activités* » de GOOGLE FRANCE, qui constitue « *l'établissement* » sur le territoire français de GOOGLE LLC et GOOGLE IRELAND LIMITED.

Au vu des manquements relevés, la CNIL a prononcé une amende de 90 millions d'euros à l'encontre de GOOGLE LLC et de 60 millions d'euros à l'encontre de GOOGLE IRELAND LIMITED, considérées comme des responsables conjoints du traitement, dès lors qu'elles déterminaient toutes les deux les finalités et les moyens dudit traitement.

La CNIL a également enjoint à ces deux sociétés d'offrir un moyen de refuser les cookies « *présentant une simplicité équivalente au mécanisme prévu pour leur acceptation* », sous astreinte de 100 000 euros par jour de retard à l'issue d'un délai de 3 mois, et a ordonné la publication de cette décision.

[Lien vers la décision](#)

LA COREE DU SUD RECONNUE « PAYS ADEQUAT »

La Commission européenne a adopté, le 17 décembre 2021, une décision d'adéquation reconnaissant que le niveau de protection des données personnelles en Corée du Sud est substantiellement équivalent à celui garanti par le droit de l'Union européenne.

Après avoir « soigneusement analysé la législation et les pratiques coréennes », la Commission européenne a estimé que la République de Corée assurait un niveau de protection adéquat des données à caractère personnel transférées d'un responsable du traitement (ou sous-traitant) dans l'Union à une entité en Corée du Sud.

Cette décision a notamment été motivée par l'existence :

- (i) d'un cadre réglementaire de protection des données (la protection des données à caractère personnel étant reconnue au niveau constitutionnel et la Corée ayant promulgué de nombreuses lois dans le domaine de la protection des données) ;
- (ii) de droits pour les personnes concernées, d'obligations pour les responsables du traitement et de garde-fous, des mécanismes de surveillance et des voies de recours permettant d'identifier et de traiter les infractions aux règles de protection des données.

La Commission ne s'est pas contentée de constater l'existence de sources juridiques, mais a également vérifié la façon dont ces mesures étaient mises en œuvre et la façon dont les données étaient utilisées par les autorités publiques.

A ce titre, la Commission considère que toute ingérence par les autorités publiques coréennes dans les droits fondamentaux des personnes ayant pour finalité l'intérêt public (finalité de répression pénale et de sécurité nationale), est limitée à ce qui est strictement nécessaire pour atteindre l'objectif légitime en question, et qu'il existe une protection juridique efficace contre une telle ingérence.

Désormais, une entreprise souhaitant transférer des données personnelles en Corée du Sud dans le cadre d'un traitement n'aura plus à recourir aux garanties appropriées telles que les Règles d'Entreprise Contraignantes (BCR) ou les Clauses Contractuelles Types (CCT).

Cette décision d'adéquation sera réévaluée par la Commission dans un délai de 3 ans suivant son entrée en vigueur, puis tous les 4 ans par la suite. La Commission européenne continuera à suivre la situation juridique en Corée et pourra, si nécessaire, décider de suspendre, de modifier ou d'abroger la décision d'adéquation, ou d'en limiter la portée.

[Lien vers la décision de la Commission Européenne](#)

CAMERA-PIETON ET VIDEOPROTECTION : UNE COMMUNE MISE EN DEMEURE PAR LA CNIL

La CNIL a mis en demeure une commune de mettre en conformité ses dispositifs de caméra-piéton et de vidéoprotection, ces derniers portant atteinte à de nombreuses obligations posées par la loi Informatique et Libertés et le Code de la sécurité intérieure.

Après avoir effectué un contrôle sur place, la CNIL a constaté que les dispositifs de vidéoprotection et de caméra-piéton, installés par une commune, contrevenaient tant au Code de la sécurité intérieure (CSI) qu'à la loi Informatique et Libertés (LIL).

En ce qui concerne les caméras-piétons, la CNIL a estimé (i) que ce dispositif contrevenait au principe d'exactitude des données en ce que l'horodatage et l'identifiant de l'agent de police municipale porteur de la caméra étaient inexacts (art 4 LIL), (ii) que ce dispositif ne respectait pas les durées de conservation dès lors que certains fichiers vidéos étaient présents depuis plus de 6 mois sur les caméras (art 87 LIL), (iii) que du fait de l'absence de mentions d'information sur le site internet ou par voie d'affichage dans la commune, les personnes concernées n'étaient pas correctement informées (art 104 LIL), (iv) que la sécurité des données n'était pas suffisante dès lors que le mot de passe d'accès à la caméra n'était pas assez robuste et qu'aucune mesure de traçabilité des accès n'était mise en œuvre (art 99 et 101 LIL), et enfin (v) que l'utilisation de la caméra-piéton n'avait pas fait l'objet d'une inscription dans le registre des traitements de la commune (art 100 LIL).

En ce qui concerne la vidéoprotection, la CNIL a estimé que ce dispositif portait atteinte au Code de la sécurité intérieure car, d'une part, il permettait la visualisation de l'intérieur d'immeubles d'habitation (art L251-3 CSI) et, d'autre part, la commune ne respectait pas la durée maximale de conservation des données (art L252-5 CSI). La CNIL a considéré par ailleurs que ce dispositif portait atteinte à la loi Informatique et Libertés dès lors qu'aucune analyse d'impact n'avait été effectuée (art 90 LIL) et car les panneaux d'information apposés à chaque entrée sur la commune ne procuraient pas une information correcte du public, les mentions obligatoires d'information étant manquantes (art 104 LIL).

En conséquence, la CNIL a mis en demeure la commune de mettre ces deux dispositifs en conformité dans un délai de 4 mois.

[Lien vers la publication de la CNIL](#)

SLIMPAY CONDAMNEE PAR LA CNIL POUR VIOLATION DE DONNEES

Le 28 décembre 2021, la CNIL a prononcé une amende d'un montant de 180 000 euros à l'encontre de SLIMPAY, en raison d'un manquement de la société à son obligation de sécurité des données personnelles de ses utilisateurs, et d'une absence de communication de la violation à ces derniers.

En 2015, à l'occasion d'un projet de recherche interne sur un mécanisme de lutte contre la fraude, SLIMPAY, établissement de paiement agréé proposant des services de paiement « SEPA », a réutilisé des données à caractère personnel contenues dans ses bases de données à des fins de test. Elle a ainsi importé des données à caractère personnel de débiteurs sur un serveur.

Lorsque le projet de recherche s'est terminé, en 2016, les données sont restées stockées sur ce serveur, qui ne faisait pas l'objet d'une procédure de sécurité particulière et qui était librement accessible depuis Internet. Etaient ainsi notamment accessibles l'état civil et les coordonnées bancaires de douze millions de débiteurs.

Alertée en 2020 par un de ses clients, SLIMPAY a, afin de mettre un terme à cette violation, « immédiatement procédé à l'isolement du serveur et à la mise sous séquestre de données » et a notifié cette violation à la CNIL.

À la suite de cette notification, la CNIL a procédé à un contrôle, au cours duquel il lui est apparu que :

- certains contrats conclus par SLIMPAY avec ses sous-traitants n'incluaient pas l'ensemble des mentions obligatoires au titre de l'article 28 du RGPD ;
- l'accès au serveur contenant les données « *n'était encadré d'aucune mesure de restriction d'accès satisfaisant* », les données n'étaient pas chiffrées et aucune mesure de journalisation n'était mise en œuvre, de sorte que les actions effectuées sur le serveur n'étaient pas détectées ;
- SLIMPAY n'a pas communiqué la violation aux personnes concernées, pourtant exposées « *au risque d'une réutilisation de leurs données à caractère personnel par des attaquants* », notamment dans le cadre d'opérations de « *phishing* »

En défense, SLIMPAY a indiqué que le projet de recherche ayant débuté en 2015, le RGPD n'était pas applicable. La CNIL a retorqué que, le défaut de sécurité ayant perduré après le 25 mai 2018, le RGPD était bien applicable audit défaut de sécurité.

La CNIL a considéré, au vu de ce qui précède, que SLIMPAY avait manqué aux obligations suivantes :

- les obligations en matière de sous-traitance prescrites par les paragraphes 3 et 4 de l'article 28 du RGPD ;
- l'obligation d'assurer la sécurité des données ;
- l'obligation de communiquer aux personnes concernées la violation de données.

La CNIL a, en conséquence, prononcé une amende administrative de 180 000 € à l'encontre de SLIMPAY et a rendu publique sa délibération.

[Lien vers la publication de la CNIL](#)

PUBLICATION D'UN GUIDE RGPD A L'ATTENTION DES DEVELOPPEURS

Après avoir élaboré une première version en janvier 2020, la CNIL a mis à jour en décembre 2021 son guide RGPD à destination des développeurs. Ce guide s'adresse à tous développeurs, qu'ils travaillent seuls ou en équipe, et plus généralement à toute personne s'intéressant au développement web ou applicatif ou en faisant son métier.

Cette nouvelle version du guide se scinde, comme la première, en différentes fiches thématiques couvrant les besoins les plus fréquents des développeurs au cours de leurs projets.

Ces fiches traitent de thématiques juridiques (le développement en conformité avec le RGPD, l'identification des données personnelles, la minimisation de la collecte de données, l'information des personnes, l'exercice des droits des personnes, des durées de conservation et la prise en compte des bases légales), mais également de thématiques techniques (la sensibilisation des développeurs à la préparation et la sécurisation de leurs développements informatiques, la gestion de leur code source et des utilisateurs, le choix de l'architecture, la sécurisation des sites, applications et serveurs, la maîtrise des bibliothèques, SDK et de la qualité du code, les tests des applications et la mesure de la fréquentation des sites web).

Cette dernière version comporte notamment deux nouvelles fiches thématiques :

- une relative à l'analyse des pratiques en matière de traceurs sur les sites et applications, rappelant les principes de base et les bonnes pratiques applicables aux cookies ; et
- une relative aux moyens de se prémunir d'une attaque informatique, en précisant les moyens classiques d'attaque d'un site (attaque par force brute, manipulation d'URL, programmes malveillants et rançongiciels...) et en fournissant des liens vers différents sites d'informations complémentaires.

Ce guide est contributif, en ce sens où toute personne peut proposer des ajouts ou modifications.

[Lien vers le guide](#)

PRECISIONS DE LA CEDH SUR LA PORTEE DU DROIT A L'OUBLI

Par un arrêt du 25 novembre dernier, la Cour Européenne des Droits de l'Homme (« CEDH ») s'est, pour la première fois, prononcée sur la compatibilité du droit à la liberté d'expression avec la condamnation civile d'un journaliste pour refus prolongé de désindexer des données sensibles relatives à des particuliers.

Un ressortissant italien, rédacteur en chef d'un journal en ligne, avait publié un article relatif à une bagarre dans un restaurant, faisant mention des noms des restaurateurs ainsi que de procédures pénales les concernant. Deux ans plus tard, les restaurateurs ont demandé au journaliste de retirer l'article du site internet. Faute de suite favorable donnée, les juridictions internes ont été saisies notamment en application du « Code de protection des données à caractère personnel » italien.

Les juridictions internes ont considéré que la demande de retrait de l'article n'avait plus lieu d'être dans la mesure où le journaliste avait, entretemps, procédé à sa désindexation. Toutefois, elles ont jugé que le journaliste avait porté atteinte à la réputation et à la vie privée des restaurateurs compte tenu de l'accès facilité en ligne (*« bien plus que toute information publiée dans les journaux imprimés, compte tenu de la large diffusion locale du journal en ligne en question »*) à des informations relatives à des procédures pénales les concernant.

Les juges nationaux ont, plus particulièrement, relevé qu'il existait des « tags » de l'article correspondant aux noms des restaurateurs. Ainsi, pendant plusieurs mois, toute personne pouvait accéder à ces données, qualifiées de sensibles, en entrant simplement le nom des restaurateurs sur le moteur de recherche concerné. Le journaliste a alors été condamné au paiement de dommages et intérêts à hauteur de 5.000 euros.

Considérant qu'une telle décision portait atteinte à son droit à la liberté d'expression (consacré à l'article 10 de la Convention européenne des droits de l'Homme, la « Convention ») et que le montant de cette condamnation était excessif, le journaliste a introduit une requête devant la CEDH.

Pour rendre sa décision, la CEDH s'est appuyée sur une pluralité de dispositions de droits internes, internationales et européennes, notamment la Directive 95/46 CE, le RGPD, la jurisprudence pertinente de la CJUE en la matière (notamment l'affaire Google Spain et Google Inc. C-131/12), les lignes directrices du CEPD sur les critères du droit à l'oubli dans le cas des moteurs de recherche dans le cadre du RGPD.

Premier enseignement intéressant de l'arrêt : la CEDH n'a pas suivi la position du journaliste selon laquelle il ne pourrait être chargé de la désindexation de l'article en cause car une telle possibilité ne serait ouverte qu'au moteur de recherche concerné. La Cour a relevé que « *la désindexation peut être effectuée par un éditeur, le « nonindexing » étant une technique utilisée par les propriétaires de sites web pour dire à un fournisseur de moteur de recherche de ne pas laisser le contenu d'un article apparaître dans [ses] résultats* » et que la constatation de la responsabilité du journaliste résultait l'absence de désindexation du moteur de recherche Internet des tags vers l'article publié. En conséquence, tant les moteurs de recherche que les administrateurs de journaux ou d'archives journalistiques accessibles en ligne (dont le journaliste) peuvent être concernés par l'obligation de désindexation des documents/données.

Ensuite, la CEDH a considéré que l'ingérence dans la liberté d'expression du journaliste, qui n'était pas contestée, visait à protéger « *la réputation ou les droits d'autrui* » et avait donc un but légitime conformément à l'article 10 de la Convention.

Restait à savoir si cette ingérence était « *nécessaire dans une société démocratique* ».

Pour ce faire, la CEDH a d'abord souligné la particularité de l'affaire : il n'était pas question de la suppression définitive de l'article litigieux ni son anonymisation, mais de sa non-désindexation « *permettant ainsi la possibilité pendant une durée jugée excessive de taper dans le moteur de recherche les noms des restaurateurs afin d'accès aux informations relatives à la procédure pénale les impliquant* ».

La Cour a alors dégagé des critères spécifiques pour apprécier l'équilibre entre liberté d'expression et droit à la réputation/vie privée^[1]:

- Le premier critère est celui de la durée pendant laquelle l'article a été mis en ligne « *en particulier à la lumière des finalités pour lesquelles les données* » des personnes concernées ont été traitées à l'origine. Sur ce point, la CEDH a relevé que si la procédure pénale évoquée était bien pendante au moment de la condamnation du journaliste, les données n'avaient pas été mises à jour depuis la survenance des événements relatés. En outre, en dépit d'une mise en demeure de retirer l'article, celui-ci est resté en ligne et facilement accessible pendant une durée de 8 mois.
- Le deuxième critère est celui de la sensibilité des données en cause. En l'espèce, la Cour a noté qu'il s'agissait d'informations sur une procédure pénale.
- Le troisième et dernier critère est la gravité de la condamnation. La CEDH a rappelé qu'il y a eu une condamnation civile et non pénale et que le montant de l'indemnité n'était pas excessif au regard des circonstances de l'espèce.

La CEDH n'avait donc pas à remettre en cause la mise en balance, telle qu'entreprise par les juges internes, entre la liberté d'expression et le droit à la vie privée consacrés par la Convention. L'absence prolongée de désindexation de l'article constituait une restriction justifiable de la liberté d'expression du journaliste, ce d'autant plus qu'aucune obligation de retirer définitivement l'article n'a été imposée.

Cette décision invite donc les éditeurs de journaux en ligne qui recourent à la technique de l'indexation sur les moteurs de recherche de leurs articles à la plus grande prudence : indexer des données identifiants un particulier peut, dans certains cas, notamment au regard de la sensibilité des données dudit particulier évoquées dans l'article concerné (relatives à une procédure pénale, données de santé, etc.), être sanctionné au titre du droit à l'oubli.

Source : CEDH 25 novembre 2021 (requête n°77419/16 – Affaire Biancardi contre Italie)

[¹] Critères différents de ceux qu'elle avait déjà établis dans son arrêt *Axel Springer AG c. Allemagne* 7 février 2012 car cette affaire portait sur la publication d'articles papiers faisant état d'une procédure pénale relative à une personne notoire au contraire de la présente affaire relative à la mise en ligne pendant une certaine durée d'un article relatif à une affaire pénale contre des particuliers.

LE PARLEMENT EUROPEEN RAPPELE A L'ORDRE PAR LE CEPD EN RAISON D'UN TRANSFERT DE DONNEES VERS LES ETATS-UNIS

Le CEPD a adressé au Parlement européen un rappel à l'ordre, le 5 janvier 2022, notamment en raison d'un transfert de données à caractère personnel vers les Etats-Unis qui n'était pas assorti de « mesures supplémentaires » conformément aux exigences de l'arrêt « Schrems II ».

Le Contrôleur européen de la protection des données (CEPD) a été informé, par des membres du Parlement européen, que ce dernier aurait commis des manquements au Règlement (UE) 2018/1725 (équivalent du RGPD pour les institutions, organes et organismes de l'UE), notamment en matière de transparence et de transferts de données personnelles.

Était en cause le recours par le Parlement européen aux services d'une société baptisée « Ecolog », qui (i) conduisait des tests PCR dans son enceinte, et (ii) éditait un site internet dédié (europarl.ecocare.center), lequel utilisait des cookies Google Analytics et Stripe.

A l'issue d'échanges avec le Parlement européen, il est apparu au CEPD que les données de membres et d'employés du Parlement européen étaient transférées aux Etats-Unis dans le cadre de l'utilisation de ces cookies. S'appuyant sur l'arrêt « Schrems II », le CEPD a rappelé que les transferts de données à caractère personnel à destination des Etats-Unis ne pouvaient avoir lieu qu'en présence de « mesures supplémentaires » permettant d'assurer un niveau de protection des données équivalent à celui de l'Union européenne. Le Parlement européen, qualifié ici de responsable du traitement, ne rapportait, cependant, aucune preuve de l'existence de telles mesures, ce qui a conduit le CEPD à conclure que le Parlement européen avait manqué à ses obligations en matière de transfert de données.

A la lumière de ces constatations, le CEPD a adressé un rappel à l'ordre au Parlement européen.

[Lien vers la décision](#)

L'ENVOI D'UN COURRIEL A UN DESTINATAIRE ERRONE DOIT-IL ETRE NOTIFIE ?

Comme chaque mois, Alexandre Fiévée tente d'apporter des réponses aux questions que tout le monde se pose en matière de protection des données personnelles, en nous appuyant sur les décisions rendues par les autorités nationales de contrôle au niveau européen. Ce mois-ci, il se penche sur une décision de la CNPD, autorité de contrôle luxembourgeoise, relative à l'envoi par un assureur d'un courriel contenant des données de santé d'un assuré à un mauvais destinataire qui s'analyse comme une violation de données justifiant une notification à l'autorité de contrôle ainsi qu'une communication à la personne concernée.

« Tous les organismes qui traitent des données personnelles doivent, rappelle la CNIL, mettre en place des mesures pour prévenir les violations de données et réagir de manière appropriée en cas d'incident. Les obligations prévues par le RGPD visent à éviter qu'une violation cause des dommages ou des préjudices aux organismes comme aux personnes concernées. »^[1] La violation de données personnelles est définie à l'article 4.12) du RGPD comme « une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données. » Il y a donc une violation de données si un incident de sécurité impliquant un traitement de données personnelles se produit et que cet incident a un impact sur l'intégrité, la confidentialité et/ou la disponibilité des données, et ce peu importe que l'incident soit d'origine malveillante ou non et qu'il se soit produit de manière intentionnelle ou non.

Rappel du principe

En cas de violation de données, l'article 33 du RGLD impose au responsable du traitement de documenter, dans un registre, les violations de données personnelles et de notifier les violations présentant un risque pour les droits et libertés des personnes à l'autorité de contrôle et, dans certains cas, lorsque le risque est élevé, aux personnes concernées. La notification à la CNIL doit intervenir dans les meilleurs délais et au plus tard 72h après que le responsable du traitement en a pris connaissance. En pratique, le point de départ de ce délai correspond au moment où le responsable du traitement a acquis « *un degré de certitude raisonnable* » qu'un incident a eu lieu et a touché des données personnelles. « *Cela implique, précise la CNIL, qu'il ait mis en place des mesures de détection des violations et qu'il mène au plus tôt des investigations permettant d'atteindre une telle certitude raisonnable. Durant cette phase d'investigation, le responsable du traitement n'est pas considéré comme ayant connaissance de la violation.* »^[2]

L'affaire

Un assuré a été informé par son assureur qu'un courriel qui lui était destiné a été adressé par erreur à un mauvais destinataire.

Ce courriel comprenait, dans le corps du texte, notamment son nom de famille, son sexe, ainsi que des indications détaillées concernant certaines pathologies, et, en pièces jointe, trois formulaires distincts relatifs aux pathologies qu'il avait déclarées auprès de son assurance. L'assuré a saisi la CNPD d'une réclamation, étant précisé que cette erreur s'est répétée une seconde fois.

Dans ce contexte, l'autorité de contrôle luxembourgeoise a décidé d'ouvrir une enquête, qui s'est traduite par un contrôle sur place dans les locaux de l'assureur.

La question qui se posait était de savoir si l'incident en question devait s'analyser comme une violation de données et, dans l'affirmative, si l'assureur aurait dû notifier la violation à la CNPD et informer le ou les personne(s) concernée(s).

Selon l'assureur, les obligations du RGPD ne s'appliquaient pas au cas d'espèce, dans la mesure où les données transmises par les deux courriers électroniques litigieux ne permettaient pas d'identifier le réclamant.

La CNPD n'a pas suivi cette analyse et a considéré que : *« l'envoi de courriers électroniques contenant des données à caractère personnel à un destinataire erroné est dès lors à qualifier de violation de données à caractère personnel du type "violation de la confidentialité", cette dernière ayant entraîné, de manière accidentelle, une divulgation de données à caractère personnel à des personnes tierces qui n'étaient pas autorisées à prendre connaissance des informations contenues dans les courriers électroniques et leurs annexes. »*^[3]

Au vu de ce qui précède et considérant que cette violation présentait un risque élevé pour les droits et libertés, la CNPD a estimé que le responsable du traitement a manqué à ses obligations (i) en ne documentant pas la violation dans son registre, (ii) en ne notifiant pas ladite violation à l'autorité de contrôle et en ne communiquant pas à la personne concernée les informations requises de l'article 34.1 du RGPD.

Enfin, la CNPD a retenu à l'encontre de l'assureur un manquement à l'obligation de sécurité, car, selon elle, *« un chiffrement par encryptage, des mots de passe ou toute technique garantissant une protection similaire selon l'état de l'art actuel et les bonnes pratiques applicables en la matière, auraient dû être appliquées aux communications en l'espèce afin de garantir un niveau de sécurité adapté aux risques d'atteinte à la vie privée de la personne concernée, surtout pour une entreprise comme celle du contrôlé »*. Partant, l'autorité de contrôle luxembourgeoise a prononcé une amende d'un montant de 135.000 euros.

Quelles recommandations ?

Chaque incident doit être documenté dans un registre, dans lequel une analyse technique et juridique doit indiquer si l'incident a un impact sur des données personnelles en termes d'intégrité, de confidentialité et/ou de disponibilité.

Dans l'affirmative, il appartient au responsable du traitement d'évaluer le risque pour les droits et libertés des personnes concernées. Cette évaluation peut reposer sur deux critères : la facilité d'identification des personnes concernées par la violation et le caractère préjudiciable de la violation pour ces personnes, étant précisé que chacun de ces critères doit être apprécié selon des valeurs : risque maximal (4), important (3), limité (2), négligeable (1).

Selon les résultats de cette évaluation, une notification s'impose si un risque important a été identifié (ex : la valeur totale des deux critères est égale à 6) ; une communication aux personnes concernées se justifie par ailleurs si un risque maximal a été identifié (ex : la valeur totale des deux critères est supérieure à 6).

Alexandre FIEVEE

Avocat associé

Derriennic associés

[1] <https://www.cnil.fr/fr/les-violations-de-donnees-personnelles>

[2] <https://www.cnil.fr/fr/les-violations-de-donnees-personnelles>

[3] Délibération n°31FR/2021, 5 août 2021

ACTUALITE EUROPEENNE :

PANORAMA DE QUELQUES DECISIONS RENDUES PAR DES AUTORITES NATIONALES DE CONTROLE



Sanction d'un service dentaire ayant permis un accès irrégulier à des

Datatilsynet (Danemark), 16 décembre 2021

Le service de soins dentaires municipal mettait en œuvre une solution logicielle permettant aux parents d'accéder aux feuilles de soins dentaires de leurs enfants. L'accès à cette solution a, par la suite, été élargi aux parents divorcés ou séparés qui avaient la garde alternée de leurs enfants.

C'est dans ce contexte que la municipalité s'est rendue compte que chaque parent avait accès aux données personnelles de l'autre parent, et ce, en dépit de l'activation de l'option permettant une non-divulgaration des données à l'autre parent.

L'autorité de contrôle a ainsi infligé à la municipalité une amende d'environ 13.450 euros considérant que la municipalité avait manqué à son obligation de sécurité en ne mettant pas en œuvre les mesures techniques et organisationnelles adéquates pour assurer un niveau de sécurité approprié au risque pour les personnes concernées.

[Lien vers le communiqué en danois](#)

Un hôpital condamné pour n'avoir pas procédé à une nouvelle analyse d'impact

Personuvernd (Islande), 29 novembre 2021



Dans un but de santé publique, l'hôpital islandais « Landspítali » est chargé, depuis 2015, d'effectuer une surveillance des maladies infectieuses et des dépistages aux frontières.

A la suite de la propagation rapide et massive du COVID-19, l'hôpital a fait appel, en juin 2020, aux services d'un sous-traitant pour effectuer des tests de dépistage COVID-19. Une analyse d'impact a alors été réalisée.

Deux mois plus tard, en août 2020, l'hôpital a annoncé qu'une partie des activités du service de pathologie et de virologie de l'hôpital serait provisoirement transférée dans les locaux du sous-traitant afin d'augmenter les capacités de dépistage du COVID-19, le temps pour l'hôpital d'améliorer ses équipements.

L'hôpital a estimé qu'il n'était pas nécessaire d'effectuer une nouvelle analyse d'impact dès lors que le traitement effectué dans les locaux du sous-traitant était similaire à celui déjà effectué dans l'enceinte de l'hôpital.

L'autorité de contrôle, à l'inverse, a estimé que l'hôpital, traitant désormais des données personnelles à l'aide des installations de son sous-traitant, donnait la possibilité à certains employés du sous-traitant d'accéder à des données supplémentaires et donc aurait dû réaliser une seconde étude d'impact.

[Lien vers le communiqué en islandais](#)

Sanction d'une société refusant de fournir la photo d'une plaque d'immatriculation

HDPa (Grèce), 5 janvier 2022



Une société autoroutière, ayant mis en place un système de vidéosurveillance permettant d'enregistrer les plaques d'immatriculation des véhicules fraudant le péage, a transmis à un automobiliste une amende.

L'automobiliste, contestant avoir franchi le péage au jour et à l'heure indiqués, a exercé son droit à l'information (article 12 du RGPD) et a demandé que la copie du registre des incidents ainsi que le matériel photographique de son véhicule lui soient fournis (droit d'accès, article 15 du RGPD).

La société a, dans un premier temps indiqué que le passage avait été enregistré par le système de vidéosurveillance du péage, mais qu'il lui était impossible de divulguer les données à un « tiers », sauf sur ordre de la justice.

L'autorité de contrôle, saisi par la personne concernée, a indiqué au responsable du traitement que dès lors qu'il a reçu une amende, l'automobiliste n'était pas un « tiers » mais une personne concernée, et qu'ainsi il avait le droit d'obtenir la confirmation que des données personnelles le concernant sont traitées ainsi que le droit d'accéder auxdites données, le refus de fournir les données étant contraire à l'article 15 du RGPD.

En réponse, la société a transmis à la personne concernée le livre des incidents, mais a indiqué que le matériel photographique ne pouvait être transmis en raison d'un problème technique.

Dans le cadre de son enquête, l'autorité de contrôle a constaté que l'affirmation de la société selon laquelle le véhicule de la personne concernée avait été enregistré était en réalité fausse, et que l'impossibilité pour la société d'accéder aux images devait s'interpréter comme une violation de données (atteinte à la disponibilité) qui aurait dû faire l'objet d'investigations complémentaires. De plus, et surtout, l'autorité a estimé que le droit d'accès n'avait pas été respecté en raison du délai tardif de la réponse.

En conséquence, l'autorité de contrôle Grec a infligé au responsable du traitement une amende d'un montant de 1.000 euros pour non-respect de l'article 12 paragraphe 1 du RGPD.

[Lien vers la décision en grec](#)

ACTUALITE DU CABINET

DERRIENNIC ASSOCIES PROPOSE UN PROGRAMME DE FORMATION DE **35 HEURES** POUR LA PRÉPARATION A LA CERTIFICATION DPO

OBJECTIF

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

COUT

3000€ HT/personne

INTERVENANT



Alexandre FIEVEE

Avocat Associé

Tél : 01.47.03.14.94

afieeve@derriennic.com

Classements

Alexandre Fieeve figure dans le classement BestLawyers dans la catégorie « Information Technology Law » (2020).

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

RENSEIGNEMENTS PRATIQUES

Prochaine session 2021/2022 :

Sur demande.

Lieu de la formation :

Au cabinet Derriennic Associés (5 avenue de l'opéra - 75001 Paris) ou en visio-conférence.

Inscription et informations :

afieeve@derriennic.com