La Newsletter dédiée à la mise en conformité au RGPD

par @DerriennicParis

DERRIENNIC ASSOCIÉS

Conformité RGPD

#NewsDerriennicRGPD 21

Madame, Monsieur,

Nous vous proposons, en ce mois de février 2020, de découvrir les actualités suivantes :

- Le Conseil d'Etat fixe le cadre applicable au droit au déréférencement ;
- Brexit : les transferts de données couverts jusqu'à fin 2020
- Vidéosurveillance dans un immeuble d'habitation : un intérêt légitime des copropriétaires ;
- La NSA rend-t-elle impossible tout transfert de données vers les Etats-Unis ?
- Cookies : La CNIL publie son projet de recommandation et lance une consultation publique.

Nous vous en souhaitons une bonne lecture.

Le Conseil d'Etat fixe le cadre applicable au droit au déréférencement

Le 6 décembre dernier, le Conseil d'Etat a rendu treize arrêts, sur la base de la décision de la CJUE du 24 septembre dernier (CJUE, 24 sept. 2019, aff. C-136/17, GC, AF, BH, ED c/ Commission nationale de l'informatique et des libertés), encadrant les conditions dans lesquelles un exploitant de moteur de recherche est tenu de faire droit à une demande de déréférencement.

En l'espèce, treize particuliers avaient saisi l'exploitant du moteur de recherche Google de demandes de déréférencement de liens renvoyant vers des pages contenant des données à caractère personnel les concernant.

Face aux refus de Google, ces particuliers avaient saisi la CNIL afin qu'elle mette en demeure Google de procéder au déréférencement des liens litigieux.

La CNIL a décidé de ne pas faire droit à ces demandes et a clôturé les plaintes.

Les 13 particuliers ont saisi le Conseil d'Etat aux fins de voir annuler les décisions de la CNIL.

Le Conseil d'Etat rappelle que, conformément à la décision de la CJUE précitée, l'exploitant de moteur de recherche, saisi d'une demande de déréférencement, est tenu de mettre en balance :

- d'une part, les droits fondamentaux de la personne concernée, et

- d'autre part, le droit à l'information des internautes.

A cette fin, le Conseil d'Etat apporte des clés d'appréciation dans la mise en balance de ces droits. Trois hypothèses sont envisagées :

i) Lorsque les liens mènent vers des données qui ne sont pas sensibles :

Le Conseil d'Etat estime que trois paramètres principaux doivent être pris en compte par l'exploitant de moteur de recherche :

- Les caractéristiques des données personnelles en cause (par exemple : leur nature, leur contenu, la date de leur mise en ligne, etc.) et les répercussions de leur référencement pour l'intéressé ;

- Le rôle social du demandeur (par exemple : son rôle dans la vie publique, sa notoriété ou encore sa profession) ; et

- Les conditions d'accès de l'information en cause (par exemple : les mots clés devant être indiqués pour y accéder, le classement du lien dans la page de résultats de la recherche, etc.) et, si l'intéressé a de lui-même rendu ces informations publiques.

ii) Lorsque les liens mènent vers des données personnelles sensibles :

Étant donné que le caractère sensible des données à caractère personnel entraîne une ingérence plus grave dans la vie privée de la personne concernée, le Conseil d'État considère que l'appréciation du droit à l'information du public doit être plus exigeante.

iii) Lorsque les liens mènent vers des données personnelles relatives à une procédure pénale :

Selon le Conseil d'Etat, il convient d'appliquer le cadre dédié aux données sensibles.

De plus, le Conseil d'Etat estime que l'exploitant d'un moteur de recherche est tenu d'organiser la liste des résultats, de manière à ce que les premiers liens référencés soient ceux qui contiennent des informations actualisées relatives à la procédure pénale, correspondant ainsi à la situation judiciaire actuelle de la personne concernée.

A noter : A la suite de ces treize arrêts, la CNIL a mis à jour sa page de réponses aux questions

(FAQ) concernant le droit au déréférencement (consultable ici).

Lien vers les décisions :

https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-6-decembre-2019-13-decisions-relatives-au-droit-a-l-oubli

Brexit : les transferts de données couverts jusqu'à fin 2020

Le 31 janvier 2020, la CNIL a émis une publication indiquant que le Royaume-Uni continuera d'appliquer le RGPD, au moins jusqu'au 31 décembre 2020.

La CNIL a publié, le 31 janvier 2020, jour de la sortie du Royaume-Uni de l'Union européenne, un texte indiquant qu'en application de l'accord de retrait, les dispositions du RGPD continueront à s'appliquer à ce pays pendant une période transitoire courant jusqu'au 31 décembre 2020. Cette période transitoire pourra faire l'objet d'une prolongation, pour une durée maximale de un à deux ans.

Pendant cette période transitoire, il ne sera pas nécessaire d'encadrer les transferts de données à caractère personnel vers le Royaume-Uni au moyen de garanties appropriées prévues par le RGPD

A l'issue de la période transitoire, les transferts de données personnelles vers le Royaume-Uni devront être encadrés par les outils prévus par le RGPD, à moins qu'une décision prise par la Commission européenne ne reconnaisse que le Royaume Uni garantit un niveau de protection adéquat. Pour rappel, la Commission européenne a d'ores et déjà évoqué la possibilité qu'une décision d'adéquation soit prise avant la fin de l'année 2020.

Lien vers la publication de la CNIL :
https://www.cnil.fr/fr/brexit-quelles-consequences-la-protection-des-donnees-personnelles-durant-la-periode-transitoire

Vidéosurveillance dans un immeuble d'habitation : un intérêt légitime des copropriétaires

La CJUE a été saisie, par une juridiction roumaine, d'une question préjudicielle portant sur la conformité d'une disposition de droit national autorisant la mise en place d'un système de vidéosurveillance dans les parties communes d'un immeuble d'habitation.

Une association de copropriétaires d'un immeuble roumain a décidé, lors d'une assemblée générale, d'installer trois caméras de surveillance dans les parties communes :

- une orientée vers la façade de l'immeuble ;
- une autre installée dans le hall du rez-de-chaussée ;
- et enfin, une dernière dans l'ascenseur.

L'un des résident a saisi les juridictions roumaines afin d'enjoindre l'association de retirer les trois caméras et de mettre celles-ci définitivement hors service. Ce résident a fait valoir que le système en cause violait le droit au respect de la vie privée.

L'association des copropriétaires a indiqué que la décision d'installer un système de vidéosurveillance avait été prise afin de contrôler aussi efficacement que possible les allées et venues dans l'immeuble, en raison du fait que l'ascenseur avait été vandalisé à de nombreuses reprises et que plusieurs appartements ainsi que les parties communes avaient fait l'objet de cambriolages et de vols, malgré la présence d'un système d'entrée dans l'immeuble avec interphone et carte magnétique.

Les faits ont eu lieu sous l'empire de la Directive 95/46/CE, aujourd'hui abrogée.

La juridiction, saisie par le résident, a sursis à statuer et a posé trois questions à la CJUE, qui les a synthétisées en une seule et même question :

> « *la juridiction de renvoi demande, en substance, si l'article 6, paragraphe 1, sous c)*[sur le caractère adéquate, pertinent et non excessif des données]*, et l'article 7, sous f)*[sur l'intérêt légitime]*, de la directive 95/46, lus à la lumière des articles 7 et 8 de la Charte, doivent être interprétés en ce sens qu'ils s'opposent à des dispositions nationales qui autorisent la mise en place d'un système de vidéosurveillance, tel que le système en cause au principal, installé dans les parties communes d'un immeuble à usage d'habitation, aux fins de poursuivre des intérêts légitimes consistant à assurer la garde et la protection des personnes et des biens, sans le consentement des personnes concernées.* »

La CJUE a, dans cette décision du 11 décembre 2019, souligné que le choix de l'intérêt légitime comme base légale d'un traitement requiert la réunion de trois conditions cumulatives :

- la poursuite de l'intérêt légitime ;
- la nécessité du traitement pour la réalisation de l'intérêt légitime ;
- le fait que les droits et libertés fondamentales de la personne concernée ne prévalent pas sur l'intérêt légitime poursuivi.

1. Sur la poursuite de l'intérêt légitime

La CJUE a relevé que l'intérêt légitime doit être né et actuel à la date du traitement, et ne pas présenter de caractère hypothétique à cette date. La CJUE tempère néanmoins cette exigence :

> « *Il ne saurait cependant être nécessairement exigé, lors de l'appréciation de l'ensemble des circonstances du cas d'espèce, qu'il ait été porté antérieurement atteinte à la sécurité des biens et des personnes.* »

En l'espèce, la CJUE a estimé que, « *dans une situation telle que celle en cause au principal, la condition relative à l'existence d'un intérêt né et actuel semble en tout état de cause être satisfaite, dès lors que la juridiction de renvoi relève que des vols, des cambriolages et des actes de vandalisme s'étaient produits avant la mise en place du système de vidéosurveillance et ce malgré l'installation, dans l'entrée de l'immeuble, d'un système sécurisé composé d'un interphone et d'une carte magnétique* ».

2. Sur la nécessité du traitement pour la réalisation de l'intérêt légitime

Pour la CJUE, la condition de nécessité du traitement impose à la juridiction de renvoi de vérifier que l'intérêt légitime du traitement des données poursuivi par la vidéosurveillance en cause au principal, ne peut raisonnablement être atteint de manière aussi efficace par d'autres moyens moins attentatoires aux libertés et aux droits fondamentaux des personnes concernées, en particulier aux droits au respect de la vie privée et à la protection des données à caractère personnel garantis par les articles 7 et 8 de la Charte.

La CJUE a considéré que cette condition est à rapprocher du principe de minimisation des données.

En l'espèce, la CJUE, qui a relevé que des mesures alternatives (interphone et carte magnétique) mises en place s'étaient révélées insuffisantes, et que le système de vidéosurveillance était limité aux seules parties communes de la copropriété et aux voies d'accès à celle-ci, a considéré que les exigences liées à la proportionnalité du traitement avaient été prises en comptes.

3. Sur l'existence de droits et de libertés fondamentaux de la personne concernée qui prévaudraient sur l'intérêt légitime

La CJUE a rappelé que l'appréciation de cette condition nécessite qu'il soit procédé à une pondération des droits et des intérêts opposés en cause en fonction des circonstances concrètes du cas particulier concerné, dans le cadre de laquelle il doit être tenu compte de l'importance des droits de la personne concernée résultant des articles 7 et 8 de la Charte.

Dans le cadre de cette pondération, il doit être tenu compte de :

- la gravité de l'atteinte aux droits et aux libertés de la personne concernée ;
- la nature des données à caractère personnel en cause (des données sensibles sont-elles traitées ?) ;
- la nature et les modalités concrètes du traitement de données en cause (notamment le nombre de personnes qui ont accès aux données et les modalités d'accès aux données) ;
- les attentes raisonnables de la personne concernée à ce que ses données à caractère personnel ne soient pas traitées lorsque, dans les circonstances de l'espèce, cette personne ne peut raisonnablement s'attendre à un traitement ultérieur de celles-ci ;

Selon la CJUE, ces éléments doivent être mis en balance avec l'importance, pour l'ensemble des copropriétaires de l'immeuble concerné, de l'intérêt légitime poursuivi en l'espèce par le système de vidéosurveillance en cause, en ce que celui-ci vise essentiellement à assurer la

protection des biens, de la santé et de la vie desdits copropriétaires.

Compte tenu de ce qui précède, la CJUE a répondu aux questions posées par la juridiction roumaine, dans ces termes : « *l'article 6, paragraphe 1, sous c), et l'article 7, sous f), de la directive 95/46, lus à la lumière des articles 7 et 8 de la Charte, doivent être interprétés en ce sens qu'ils ne s'opposent pas à des dispositions nationales qui autorisent la mise en place d'un système de vidéosurveillance, tel que le système en cause au principal installé dans les parties communes d'un immeuble à usage d'habitation, aux fins de poursuivre des intérêts légitimes consistant à assurer la garde et la protection des personnes et des biens, sans le consentement des personnes concernées, si le traitement de données à caractère personnel opéré au moyen du système de vidéosurveillance en cause répond aux conditions posées audit article 7, sous f), ce qu'il incombe à la juridiction de renvoi de vérifier*. »

Lien vers la décision :
http://curia.europa.eu/juris/document/document.jsf;jsessionid=D7C5474819384391A81D7251D027BADB?text=&docid=221465&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=7396762

La NSA rend-t-elle impossible tout transfert de données vers les Etats-Unis ?

La Cour de justice de l'Union européenne (CJUE) a été saisie de la question de savoir si les transferts de données à caractère personnel vers les Etats-Unis, n'étaient pas contraires à la Charte des droits fondamentaux de l'Union européenne, même lorsque ces transferts sont couverts par des clauses contractuelles types, compte tenu des atteintes à la vie privée causées par la surveillance massive et indiscriminée pratiquée par la NSA. L'avocat général de la CJUE a rendu ses conclusions sur le sujet, le 19 décembre 2019 (affaire 311/18).

Un particulier autrichien, utilisateur de Facebook, a saisie l'autorité de contrôle irlandaise (le DPC) d'une plainte par laquelle il lui demandait, en substance, d'interdire à Facebook Ireland de transférer les données à caractère personnel le concernant vers les Etats-Unis. Il faisait valoir le fait que le droit et les pratiques en vigueur aux Etats-Unis ne garantissent pas une protection suffisante contre les intrusions découlant des activités de surveillance pratiquées par les autorités publiques, notamment la National Security Agency (NSA).

Le DPC a estimé que le droit américain n'offrait pas de voies de recours effectives au sens de l'article 47 de la Charte des droits fondamentaux de l'Union européenne aux citoyens de l'Union dont les données sont transférées aux Etats-Unis, où elles risquent d'être traitées par des agences américaines à des fins de sécurité nationale, d'une manière incompatible avec les articles 7 (« Respect de la vie privée et familiale) et 8 (« Protection des données à caractère personnel) de ladite Charte. Le DPC a relevé que les clauses contractuelles types (CCT) sont inefficaces à cet égard, car elles lient seulement l'exportateur et l'importateur, mais pas les autorités ou agences américaines.

Le DPC a engagé une procédure devant la juridiction de renvoi, à savoir la High Court, visant à ce que cette dernière, si elle partage les doutes du DPC, saisisse la CJUE d'un renvoi préjudiciel sur la validité de la décision d'adoption, par la Commission européenne, des CCT.

La juridiction de renvoi a relevé plusieurs éléments qui lui font dire que les Etats-Unis procèdent à « des traitements massifs et indiscriminés de données à caractère personnel qui pourraient exposer les personnes concernées à un risque de violation des articles 7 et 8 de la Charte » :

- la NSA peut accéder aux données passant par les câbles sous-marins, avant même que lesdites données n'arrivent aux Etats-Unis ;

- les activités de la NSA ne sont pas régies par la loi ;

- les activités de la NSA ne font pas l'objet d'une surveillance judiciaire ;

- les activités de la NSA ne sont pas susceptibles de recours juridictionnel.

Dans ce cadre, la High Court a décidé de surseoir à statuer et a notamment posé à la CJUE la question suivante :

La décision 2010/87, portant adoption des CCT par la Commission européenne, est-elle valide au regard des articles 7, 8 et 47 de la Charte, dans la mesure où elle ne lie pas les autorités des Etats tiers (type NSA) ?

Dans ses conclusions, l'avocat général a relevé que les CCT peuvent être « amenuisées, voire annihilées, lorsque le droit du pays tiers de destination impose à l'importateur des obligations contraires à ce que requièrent ces clauses ».

Pour l'avocat général, il incombe au responsable du traitement et à l'autorité de contrôle d'examiner le droit du pays tiers, afin de déterminer s'il fait obstacle à l'exécution des CCT : «c'est au cas par cas, pour chaque transfert spécifique, que le responsable du traitement ou, à défaut, l'autorité de contrôle, examinera si le droit du pays tiers de destination fait obstacle à l'exécution des clauses contractuelles types et, partant, à une protection appropriée des données transférées».

Selon l'avocat général, si l'importateur se trouve dans l'incapacité de se conformer à ces clauses, il accepte d'en informer dans les meilleurs délais l'exportateur, auquel cas ce dernier a le droit de suspendre le transfert et/ou de résilier le contrat. Pour l'avocat général, le fait qu'il s'agisse d'un « droit » de suspendre le transfert et/ou de résilier le contrat ne porte pas préjudice à l'obligation de l'exportateur « de procéder ainsi au regard des exigences de protection des droits des personnes concernées découlant du RGPD ».

Par ailleurs, les autorités de contrôles sont tenues d'examiner les plaintes introduites par une personne dont les données sont transférées vers un Etats tiers en méconnaissance des CCT applicables au transfert. Le constat d'adéquation opéré dans la décision « Privacy Shield » ne prive pas les autorités de contrôle du pouvoir de suspendre ou d'interdire un transfert de données vers les Etats-Unis exécuté en vertu des CCT.

Pour l'avocat général, la validité de la décision 2010/87 « ne dépend pas du niveau de protection existant dans chaque pays tiers vers lesquels des données pourraient être transférées sur le fondement des CCT qu'elle énonce ».

En conséquence, l'avocat général n'a relevé aucun élément de nature à affecter la validité de la décision 2010/87 au regard des articles 7, 8 et 47 de la Charte.

Enfin, l'avocat général a émis, concernant la conformité de la décision « Privacy Shield », des observations, qui se bornent « à fournir certaines réflexions qui pourraient se révéler utiles à la Cour dans l'hypothèse où elle souhaiterait, contrairement à ce que [l'avocat général] préconise, statuer sur ce point ». Il relève ainsi que cette décision ne fait « pas apparaitre que les mesures de surveillance fondées sur l'EO 12333 seraient notifiées aux individus concernés ou encadrées par des mécanismes de contrôle juridictionnel ou administratif indépendant à un quelconque stade de leur adoption ou de leur mise en œuvre » et que l'institution du médiateur ne fournit pas, à son sens, une voie de recours devant un organe indépendant offrant une possibilité de faire valoir leur droit d'accès aux données ou de contester d'éventuels manquements aux règles applicables de la part des services de renseignement.

A vu de ce qui précède, l'avocat général a affirmé nourrir « certains doutes sur la conformité de la décision "Bouclier de protection des données" à l'article 45, paragraphe 1, du RGPD, lu à la lumière des articles 7,8 et 47 de la Charte ainsi que de l'article 8 CEDH ».

Lien vers la décision :
https://www.doctrine.fr/d/CJUE/2019/CJUE62018CC0311?q=311%2F18&position=3&query_key=889565da77e20b883df26bd259b7f3b7&original_query_key=889565da77e20b883df26bd259b7f3b7&source=excerpt_results

Cookies : La CNIL publie son projet de recommandation et lance une consultation publique

Le 14 janvier dernier, la CNIL a publié un projet de recommandation de mise en œuvre pratique de ses lignes directrices du 4 juillet 2019 relatives aux cookies et autres traceurs.

Pour mémoire, en juillet dernier, la CNIL mettait fin aux pratiques visant à considérer que la poursuite de navigation valait consentement des internautes et réaffirmait l'obligation des acteurs du secteur d'être à même de prouver l'obtention d'un consentement valide des internautes.

Le projet du régulateur contient 9 articles comportant (i) des recommandations, (ii) des exemples de mentions d'information et (iii) des exemples de bonnes pratiques opérationnelles de mise en œuvre de ses lignes directrices.

Tout d'abord, la CNIL propose des recommandations pratiques permettant de recueillir un consentement valide des internautes (c'est-à-dire un consentement « éclairé », « libre », « spécifique » et « univoque »).

A titre d'exemples, le régulateur propose :

- De faire figurer sur l'écran des internautes, avant même de recueillir leur consentement, les finalités des cookies ainsi qu'un court descriptif de ces finalités puis, en complément, un descriptif plus détaillé devant être accessible depuis l'interface permettant de recueillir le consentement des internautes ;

- De communiquer la liste exhaustive de tous les responsables de traitement au moment du recueil du consentement et « de manière permanente » à un endroit « aisément accessible »;

- De ne pas utiliser des pratiques de conception qui tendraient notamment à donner l'impression aux internautes que leur consentement est obligatoire pour la poursuite de la navigation (prohibition du « cookie wall ») ;

- De permettre aux internautes de consentir « finalité par finalité » et, quand la possibilité d'accepter globalement l'ensemble des finalités des cookies leur est offerte, d'être en mesure de refuser globalement les finalités de ces cookies ;

- Le cas échéant, d'enregistrer le refus des internautes au même titre que leur consentement, afin de ne pas solliciter à nouveau ce consentement « pendant un certain laps de temps ».

Ensuite, la CNIL propose aux responsables de traitement de mettre en œuvre des mécanismes permettant de prouver le recueil du consentement des internautes (par exemple par des traceurs et par l'horodatage du consentement), ainsi que la preuve de la validité de ce consentement (notamment par la mise sous séquestre du code informatique auprès d'un tiers, par des captures d'écran ou encore par des audits réguliers).

Aussi, afin d'assurer une meilleure transparence lors de l'usage des cookies, la CNIL propose plusieurs bonnes pratiques relatives à l'utilisation des cookies (par exemple en utilisant des cookies différents pour chaque finalité distincte, en utilisant des noms explicites et uniformisés pour les traceurs, etc.).

Enfin, la CNIL émet des recommandations à destination des développeurs de navigateurs et des systèmes d'exploitation qui souhaiteraient intégrer des mécanismes de recueil du consentement des utilisateurs pour ensuite transmettre aux éditeurs de sites et

d'applications mobiles les préférences des utilisateurs (par exemple en s'assurant du caractère éclairé du choix des internautes et que le recueil du consentement est conforme à la réglementation).

Ce projet de recommandation fait actuellement l'objet d'une consultation publique, ouverte jusqu'au 25 février prochain, pour une publication de la version définitive prévue au mois de mars 2020. Les professionnels auront ensuite 6 mois pour se mettre en conformité.

Pour leur part, les professionnels de la publicité en ligne s'indignent et craignent un « scenario catastrophe » pour l'écosystème, du fait d'une lourde diminution du taux d'acceptation des cookies. Ils estiment, en effet, que ce taux d'acceptation, aujourd'hui évalué à 70%, atteindrait 10% une fois les recommandations mises en œuvre.

Lien vers le projet de recommandation :
https://www.cnil.fr/sites/default/files/atoms/files/projet_de_recommandation_cookies_et_autres_traceurs.pdf