LA LETTRE DU CABINET

DONNEES PERSONNELLES

Edito

Nous avons le plaisir de vous adresser le troisième numéro de notre lettre « Données Personnelles ».
Cette lettre a pour objet de vous informer sur les développements réglementaires et jurisprudentiels en matière de protection des données personnelles, plus particulièrement concernant la mise en œuvre du RGPD en France et dans l'Union européenne.

Cette lettre « Données personnelles » est organisée autour des thématiques suivantes : les évolutions réglementaires, la conformité au RGPD, la jurisprudence, la sécurité et une partie internationale.

N'hésitez pas à diffuser cette newsletter à vos collègues et contacts !

Si vous le souhaitez, merci de nous faire part de vos impressions, critiques ou suggestions.

Bonne lecture !

* Nous poursuivons par ailleurs la publication régulière de notre newsletter sur le droit des technologies.

Sommaire

Réglementation

Dans cette rubrique, nous abordons les questions relatives à la réglementation, française (loi Informatique et Libertés) et européenne (RGPD), ainsi que les avis et recommandations publiés par la CNIL

Ciblage publicitaire – La CNIL publie de nouvelles lignes directrices en matière de cookies

Dans l'attente d'un nouveau règlement e-privacy, toujours en cours de débats au niveau communautaire, la CNIL a adopté de nouvelles lignes directrices relatives aux cookies, et autres traceurs. L'objet de ces lignes directrices, qui abrogent une précédente recommandation du 5 décembre 2013, est de donner un cadre réglementaire à l'utilisation des cookies, conforme au RGPD, à l'article 82 de la loi Informatique et Libertés modifiée, et à la directive Vie privée et communications électroniques de 2002 (directive e-privacy).

Les « lignes directrices cookies » de la CNIL sont d'application très large, puisqu'elles s'appliquent à tous types d'opérations impliquant l'utilisation de cookies et autres traceurs (cookies sur tous dispositifs tels que smartphones, tablettes, ordinateurs, et autres objets connectés à internet (consoles de jeux, télévision, véhicule, assistant vocal).

Le RGPD, a renforcé la notion de consentement. Désormais, la simple poursuite de la navigation sur un site ne peut plus être considérée comme l'expression valide du consentement de l'utilisateur au dépôt de cookies. Celui-ci doit être manifesté de manière :

- *libre* : possibilité de donner ou retirer son consentement à tout moment, et de visiter un site web même en cas de refus des cookies. Le blocage au site en cas de refus des cookies (« cookie walls ») n'est pas conforme au RGPD ;
- *spécifique* : le consentement doit être donné de façon indépendante et spécifique pour chaque finalité distincte. L'acceptation des CGU ne vaut pas recueil du consentement pour les cookies ;
- *éclairée* :l'utilisateur doit être informé dans des termes simples et compréhensibles pour tous. Le renvoi vers les CGU n'est pas suffisant ; et
- *univoque* : le consentement doit se manifester par une action positive de l'utilisateur, préalablement informé.

En pratique, on s'éloigne donc de la pratique du consentement passif par la simple poursuite de la navigation sur un site web. Le consentement doit être donné de manière informée et positive, en cochant une case.

Par ailleurs, les opérateurs qui exploitent des cookies et traceurs devront être en mesure de prouver le recueil du consentement des utilisateurs, conformément à l'article 7 du RGPD.

Ces « lignes directrices cookies » seront complétées par une nouvelle recommandation de la CNIL précisant les modalités pratiques du recueil du consentement, devant être publiée au premier trimestre 2020. Les opérateurs disposeront alors d'une période de six mois pour se mettre en conformité avec ces lignes directrices.

(Délibération n°2019-093 du 4 juillet 2019 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture ou écriture dans le terminal d'un utilisateur (notamment aux cookies et autres traceurs)

Santé – La CNIL publie un référentiel sur la gestion des vigilances sanitaires

Dans le cadre de sa fonction normative, la CNIL a publié le 18 juillet dernier, un nouveau référentiel, conforme au RGPD, relatif aux traitements de données personnelles mis en œuvre à des fins de vigilance sanitaire.

Ce référentiel unique, applicable à l'ensemble des activités de vigilance sanitaire, a été élaboré suite à une concertation auprès de l'Institut national des données de santé (INDS) et plusieurs organismes publics et privés représentatifs. En effet, le système des vigilances sanitaires fonctionne sur des bases communes (même type de finalité, catégories de données traitées, destinataires). Les activités de vigilance sanitaire couvertes par ce référentiel sont la pharmacovigilance, l'addictovigilance, la biovigilance, la cosmétovigilance, etc.

Si les traitements mis en œuvre par les organismes respectent toutes les exigences du référentiel, ceux-ci peuvent procéder à une simple déclaration de conformité en ligne. En revanche, les organismes qui souhaitent s'écarter du référentiel devront continuer à demander une autorisation préalable à la CNIL.
Les traitements de données mis en œuvre par les professionnels, les établissements de santé et les agences sanitaires ne sont pas concernés par ce référentiel.
(Référentiel relatif aux traitements de données à caractère personnel mis en œuvre à des fins de gestion des vigilances sanitaires)

Privacy Shield – Troisième revue annuelle concluante
Le Privacy Shield ou Bouclier de protection des données, l'accord conclu entre la Commission européenne et la FTC américaine (Federal Trade Commission) en 2016 fait l'objet d'une revue annuelle de conformité. Le 23 octobre dernier, la Commission a publié son troisième rapport, confirmant le respect des engagements des autorités américaines en vertu de cet accord. Les Etats-Unis continuent donc à fournir un niveau de protection adéquat en cas de transfert de données personnelles de sociétés européennes vers les sociétés américaines adhérentes. Ce rapport a pour effet de renouveler le Privacy Shield pour une année supplémentaire.
La Commission a toutefois relevé quelques points à améliorer, comme la durée de la procédure de renouvellement des accréditations des sociétés participant au système, le renforcement des contrôles des entreprises n'ayant jamais sollicité d'accréditation ou le partage d'information avec la Commission et les autorités de contrôle nationales, concernant les enquêtes en cours.
Pour rappel, le Privacy Shield ne s'applique qu'aux entreprises américaine adhérentes au système, et non à l'intégralité des entreprises américaines. A ce jour, 5.000 sociétés américaines adhèrent au Privacy Shield.
(Final report from the Commission to the European Parliament and the Council on the third annual review of the functioning of the EU-U.S. Privacy Shield, Brussels, 23.10.2019 COM(2019) 495)

PLF 2020 – Projet de collecte de données sur les réseaux pour identifier les comportements frauduleux
Le 12 septembre 2019, la CNIL a publié un avis relatif au projet du gouvernement de permettre à l'administration fiscale et des douanes de collecter des données à caractère personnel publiées sur des plateformes internet par les utilisateurs (telles que Facebook, Airbnb, Leboncoin, etc.). Ce projet, qui figure à l'article 57 du projet de loi de finance pour 2020 a pour objet d'améliorer la lutte contre la fraude fiscale. L'exposé des motifs de cet article stipule la proposition *« d'autoriser l'administration à collecter en masse et exploiter, au moyen de traitements informatisés n'utilisant aucun système de reconnaissance faciale, les données rendues publiques par les utilisateurs des réseaux sociaux et des plateformes de mise en relation par voie électronique, lui permettant de mieux détecter des comportements frauduleux sans créer d'obligation déclarative nouvelle pour les contribuables et les opérateurs économiques*. »
Bien que ne remettant pas en cause le caractère légitime des objectifs poursuivis par l'administration, la CNIL a cependant émis plusieurs réserves afin de « *préserver un strict équilibre entre l'objectif de lutte contre la fraude fiscale et le respect des droits et libertés des personnes concernées.* » Selon la Commission, il convient d'évaluer le respect du principe de proportionnalité par les administrations. Ainsi, seules les données nécessaires à la fraude doivent être exploitées. A noter qu'il s'agit d'un dispositif expérimental prévu pour une durée de trois ans.
(Projet de loi de finances 2020 : publication de l'avis de la CNIL sur l'expérimentation permettant la collecte de données sur les plateformes en ligne, CNIL, 30 septembre 2019)

Conformité au RGPD/GDPR

Sous cette rubrique, nous faisons un point sur les questions relatives à la conformité au RGPD, sur les mises en demeure de la CNIL à différents organismes sur des questions de non-conformité au RGPD et sur la jurisprudence des tribunaux relative à l'application du RGPD et de la loi Informatique et Libertés

RGPD – 30% des entreprises européennes non conformes
Selon une étude menée entre les mois d'avril et juin 2019 par European Business Awards auprès de plus de 950 PME et PMI de 34 pays européens pour le compte du cabinet RSM, 30% des entreprises européennes ont déclaré ne pas être conformes au RGPD. 57% des entreprises estiment par ailleurs en respecter les règles.

De nombreuses entreprises ne comprennent pas encore les règles du RGPD, telles que la notion de consentement, le contrôle des données personnelles par les salariés, etc.
En revanche, l'accent mis par le RGPD sur la sécurité est perçu comme un point positif, ainsi que la notion de confiance des utilisateurs.
Enfin, plus d'un tiers des répondants ont souligné le coût induit par la mise en conformité au RGPD et les difficultés accrues dans les échanges avec des entreprises non-européennes.
("30% of European businesses are still not compliant with GDPR", RSM, 22 juillet 2019)

Travail – La CNIL rappelle les règles applicables à l'enregistrement vidéo ou la capture d'écran couplés à l'enregistrement des conversations téléphoniques au travail
Des employeurs souhaitent enregistrer les actions informatiques (captures d'écran ou vidéo) de leurs employés, couplées à leurs conversations téléphoniques avec des clients ou prestataires, à des fins de formation ou d'évaluation. Cette pratique, considérée comme très intrusive, est encadrée. La CNIL vient d'en rappeler les règles.
La capture d'écran couplée à l'enregistrement des conversations téléphoniques n'est pas autorisée. Selon la CNIL, une capture d'écran n'est ni pertinente, ni proportionnée car *« il s'agit d'une image figée d'une action isolée de l'employé, qui ne reflète pas fidèlement son travail*. »
En revanche, l'enregistrement d'une conversation téléphonique couplée avec l'enregistrement vidéo de l'écran est autorisé, s'il est réalisé dans le cadre professionnel, pour le seul objectif de formation du personnel et sous réserve de la mise en place d'un certain nombre de garanties, dont notamment :

- L'information des employés,
- l'enregistrement n'est actif que pendant un appel téléphonique,
- l'enregistrement ne concerne que les personnes ayant un besoin de formation et le nombre d'enregistrements doit rester proportionné au besoin de formation,
- les employés ne peuvent être formés que sur la base de leurs propres enregistrements vidéo, sauf si la vidéo est anonymisée.

Ce dispositif n'est pas adapté à d'autres finalités que la formation (évaluation du personnel, lutte contre la fraude en interne, etc.).
Par ailleurs, si l'employeur a désigné un Délégué à la protection des données (DPO), celui-ci doit être associé à la mise en oeuvre des écoutes ou des enregistrements des appels. Enfin, le dispositif doit être inscrit au registre des activités de traitement tenu par l'employeur.
(L'enregistrement vidéo ou la capture d'écran couplé à l'enregistrement des conversations téléphoniques au travail, CNIL, 17 septembre 2019)

Actions des autorités (CNIL, CEPD)

Analyse d'impact – La CNIL publie une liste des traitements pour lesquels une analyse d'impact n'est pas requise
Après avoir publié, en novembre 2018, la liste des traitements pour lesquels une analyse d'impact (AIPD ou PIA) est obligatoire, la CNIL vient de publier une liste de traitements pour lesquels une analyse d'impact n'est pas nécessaire. Cette liste a préalablement été soumise au Comité européen de la protection des données (CEPD) afin d'assurer sa cohérence avec celles des autorités de contrôle des autres Etats-membres.
La CNIL a ainsi identifié douze types de traitements pour lesquels une analyse d'impact n'est pas obligatoire, dont :

- Les traitements mis en oeuvre uniquement à des fins de ressources humaines (gestion du personnel des organismes inférieur à 250 personnes, à l'exception du profilage). Exemple : gestion de la paye, des formations, contrôle du temps de travail.
- Les traitements de gestion de la relation fournisseurs. Exemple : gestion des contrats, des commandes, etc.
- Les traitements de données de santé par un médecin exerçant à titre individuel. Exemple : gestion des rendez-vous, des dossiers médicaux, etc.

Cette liste n'est pas exhaustive. Des traitements qui n'y figurent pas peuvent ne pas nécessiter une analyse d'impact s'ils ne présentent pas un risque élevé pour les droits et libertés des personnes concernées.
A contrario, le RGPD impose de réaliser une analyse d'impact chaque fois qu'un nouveau traitement présente un risque élevé pour les droits et libertés des personnes concernées, tel un traitement de données sensibles par exemple.
(Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données n'est pas requise, CNIL, 22 octobre 2019)

Collectivités territoriales – La CNIL publie un guide d'aide à la mise en conformité
Les collectivités territoriales traitent d'importants volumes de données à caractère personnel (état civil, listes électorales, inscriptions aux écoles, etc.). A ce titre, elles doivent également se mettre en conformité au RGPD. Or, plus de 22.000 communes, soit plus de 60% des communes en France, en majorité des petites et moyennes collectivités, ne sont toujours pas en conformité, souvent par manque de moyens et de ressources dédiées.
La CNIL a donc décidé de publier un guide à leur attention afin de les accompagner dans cette démarche. Ce guide rappelle les grands principes du RGPD, indique les réflexes à acquérir et comprend un plan de mise en conformité (dont la nomination d'un DPO) et des fiches pratiques. Des fiches techniques sont également mises en ligne sur le site de la CNIL permettant d'apporter des réponses aux questions que se posent les collectivités.
(Collectivités territoriales : la CNIL publie un guide de sensibilisation au RGPD, CNIL, 18 septembre 2019)

Reconnaissance faciale – La CNIL publie une contribution
La reconnaissance faciale est de plus en plus utilisée, notamment par la vidéosurveillance, dans certaines villes ou par certains gouvernements, par les douanes lors des passages de frontières, mais également de plus en plus sur internet. Afin d'éviter des dérives sécuritaires ou des utilisations abusives par les éditeurs de sites web, la CNIL vient de publier une contribution. Ce document poursuit quatre objectifs :

- Présenter, techniquement, ce qu'est la reconnaissance faciale et à quoi elle sert. Les différentes utilisations de la reconnaissance faciale ne soulèvent pas toutes les mêmes enjeux, notamment en termes de contrôle des personnes sur leurs données ;
- Mettre en lumière les risques technologiques, éthiques, sociétaux, liés à cette technologie. L'une des caractéristiques de la reconnaissance faciale est de permettre le traitement de données à distance, le cas échéant à l'insu des personnes. Par ailleurs, le renforcement de la surveillance permis par la reconnaissance faciale peut entraîner une réduction de l'anonymat des citoyens dans l'espace public ;
- Rappeler le cadre s'imposant aux dispositifs de reconnaissance faciale et à leurs expérimentations. Les dispositifs biométriques sont encadrés plus strictement tant au niveau européen (RGPD et directive police-justice) que français (modifications de la loi Informatique et Libertés en 2018) afin d'adapter le niveau de protection des données aux nouveaux usages du numérique.
- Préciser le rôle de la CNIL dans l'éventuel déploiement, à titre expérimental, de nouveaux dispositifs de reconnaissance faciale (missions de conseil et de contrôle).

(« Reconnaissance faciale : pour un débat à la hauteur des enjeux », CNIL, 15 novembre 2019)

Mises en demeure pour non-conformité

Les procédures de mise en demeure sont l'un des moyens dont dispose la CNIL pour rappeler les organismes à leurs obligations, notamment en matière de sécurité des données. Les mises en demeure seront suivies par une procédure par la formation restreinte de la CNIL, pouvant aller jusqu'au prononcé d'une amende administrative. Toutefois, en cas de mise en conformité dans les délais impartis, la mise en demeure peut être clôturée.

Vidéosurveillance – Clôture de la mise en demeure à l'encontre de l'association « 42 »
En octobre 2018, suite à un contrôle sur place, la CNIL avait identifié plusieurs points de non-conformité au RGPD, concernant principalement le système de vidéosurveillance. La CNIL avait mis en demeure l'association 42 (école 42) de faire les corrections nécessaires.
Les points soulevés concernaient :

- Le fait que les caméras de vidéosurveillance filmaient en continu les postes de travail, les bureaux des étudiants et les espaces de détente, ce que la CNIL considère comme non justifié et disproportionné. L'école 42 a donc retiré ou réorienté les caméras ;
- Le fait que les étudiants pouvaient télécharger une application pour accéder aux images de certaines caméras. Selon la CNIL « *l'accès aux images issues du système de vidéosurveillance doit être strictement réservé aux personnes habilitées au regard de leur fonction, par exemple, les agents en charge de la sécurité ou certains membres du personnel administratif.* » Désormais, les étudiants et le personnel non autorisé ne peuvent plus avoir accès aux images issues de la vidéosurveillance ;

- Enfin, la CNIL avait identifié la faiblesse des mots de passe permettant aux agents de sécurité et aux étudiants d'accéder à la vidéosurveillance. La politique des mots de passe a été revue et renforcée.

En conséquence, la CNIL a décidé de clôturer la mise en demeure à l'encontre de l'école 42.
(*Clôture de la décision de mise en demeure n°2018-041 à l'encontre de l'Association "42", CNIL, 22 juillet 2019*)

Jurisprudence

Responsable du traitement - L'usage du bouton « j'aime » de Facebook par des sites tiers peut engager leur responsabilité
Le bouton « j'aime » de Facebook, placé sur des sites tiers, transmet des données à caractère personnel à Facebook, qui connaît ainsi les sites web visités par les internautes.
Cette affaire concernait le site allemand Fashion ID, site de vente de vêtements en ligne, accusé par une association de consommateurs allemande de transmettre des données personnelles de ses utilisateurs à Facebook, sans leur consentement.
Le 29 juillet 2019, la Cour de justice de l'Union européenne (CJUE) a décidé que les sites tiers étaient responsables conjointement avec Facebook pour la collecte et la transmission de ces données à Facebook. Par contre, les sites tiers ne sont pas responsables des traitements ultérieurs des données par Facebook. En effet, le placement du bouton « j'aime » sur leur site leur permet notamment d'optimiser la publicité pour leurs produits ou services en les rendant plus visibles sur Facebook lorsqu'un visiteur clique sur le bouton.
En conséquence, les sites doivent recueillir le consentement éclairé des visiteurs et les informer de la collecte et de la transmission de leurs données à Facebook.
(CJUE, 2é ch., aff. C-40/17, Fashion ID GmbH & Co KG c. Verbraucherzentrale NRW c.V., 29 juillet 2019)

Droit à l'oubli – Le déréférencement limité aux extensions européennes de Google
Le 24 septembre 2019, la Cour de justice de l'Union européenne (CJUE) a rendu un arrêt, à rebours de la position de la CNIL.
Alors que la CNIL considérait que les demandes de déréférencement devaient s'appliquer à l'ensemble des extensions de Google (.com, .fr, .de, etc.), la CJUE a limité la portée de ce droit aux extensions européennes. Google s'opposait à un déréférencement global et proposait de mettre en place un système de déréférencement par géoblocage, en fonction de l'adresse IP de l'internaute. Cette position avait été rejetée par la CNIL. Suite au recours de Google devant le Conseil d'Etat, celui-ci avait posé une question préjudicielle à la CJUE.
Selon la Cour, l'exploitant d'un moteur de recherche « *est tenu d'opérer ce déréférencement non pas sur l'ensemble des versions de son moteur, mais sur les versions de celui-ci correspondant à l'ensemble des États membres, et ce, si nécessaire, en combinaison avec des mesures qui, tout en satisfaisant aux exigences légales, permettent effectivement d'empêcher ou, à tout le moins, de sérieusement décourager les internautes effectuant une recherche sur la base du nom de la personne concernée à partir de l'un des États membres d'avoir, par la liste de résultats affichée à la suite de cette recherche, accès aux liens qui font l'objet de cette demande.* » La Cour rappelle par ailleurs que le droit de la protection des données n'est pas un droit absolu. Il doit être mis en balance avec d'autres droits fondamentaux (tels que le droit à l'information), conformément au principe de proportionnalité.
(CJUE, aff. C-507/17, grande chambre, Google LLC c. CNIL, 24 septembre 2019)

Données sensibles – L'interdiction de traiter des données sensibles s'applique aux moteurs de recherche
Dans un second arrêt rendu le 24 septembre 2019, la Cour de justice de l'Union européenne apporte d'importantes précisions sur les conditions dans lesquelles les personnes peuvent obtenir le déréférencement d'un lien apparaissant dans un résultat de recherche, lorsque la page à laquelle le lien renvoie contient des informations relatives à des informations sensibles les concernant. La Cour a ainsi retenu que l'interdiction de traiter des données sensibles s'applique aux moteurs de recherche.
Cette affaire concernait quatre personnes pour lesquelles les résultats litigieux avaient été obtenus à partir de leurs noms. La Cour rappelle que les moteurs de recherche sont responsables du référencement sur leurs pages.
Le moteur de recherche *« doit, sur la base de tous les éléments pertinents du cas d'espèce et compte tenu de la gravité de l'ingérence dans les droits fondamentaux de la personne concernée au respect*

de la vie privée et à la protection des données à caractère personnel, consacrés aux articles 7 et 8 de la Charte, vérifier, au titre des motifs d'intérêt public important visés à l'article 8, paragraphe 4, de ladite directive et dans le respect des conditions prévues à cette dernière disposition, si l'inclusion de ce lien dans la liste de résultats, qui est affichée à la suite d'une recherche effectuée à partir du nom de cette personne, s'avère strictement nécessaire pour protéger la liberté d'information des internautes potentiellement intéressés à avoir accès à cette page web au moyen d'une telle recherche, consacrée à l'article 11 de la Charte. »
Une fois encore, le droit au déréférencement doit être mis en balance avec les autres droits fondamentaux, tels que le droit à l'information.
(CJUE, aff. C-136/17, grande chambre, GC, AF, BH, ED c. CNIL, 24 septembre 2019)

Cookies – Arrêt de la Cour de justice de l'Union européenne sur le consentement
Dans un arrêt du 1er octobre 2019, la CJUE a rappelé les principes applicables aux cookies en matière de consentement.
Cette affaire concernait une opération de loterie pour laquelle les participants devaient cocher une case pour accepter les emails marketing, et accepter les cookies (case pré-cochée qu'ils pouvaient toutefois décocher).
Selon la CJUE, le consentement ne peut être obtenu par des cases pré-cochées. Le consentement doit être libre, spécifique, éclairé et univoque (art. 13 du RGPD). Le fait de décocher une case pour exprimer un refus ne correspond pas à un consentement éclairé. Par ailleurs, le consentement doit être univoque, c'est-à-dire qu'il doit s'appliquer aux traitements spécifiques concernés. L'utilisateur doit notamment être informé de la finalité des cookies, de leur durée et si des tiers (destinataires) ont accès aux données.
D'une manière générale, les sites web devront détailler la liste des cookies, leur finalité (marketing, ciblage, analytique) et leur durée (ou les critères permettant de définir la durée de conservation des données) et requérir le consentement des utilisateurs, sauf pour les cookies nécessaires à l'utilisation technique du site ou à la fourniture des services à l'utilisateur. En revanche, la Cour n'impose pas d'identifier les destinataires des données collectées via les cookies. L'identification des catégories de destinataires suffit.
On notera que cette décision a été rendue quelques jours après la publication par la CNIL de sa recommandation sur les cookies (voir plus haut).
(CJUE, aff. C-673-17, Planet 49 GmbH c. Bundesverband des Verbraucherzentralen und Verbraucherverbände - Verbraucherzentralen Bundesverband e.V., 1er octobre 2019)

Collecte de données – Les données collectées en violation du RGPD ne peuvent être exploitées
Une société de droit canadien, Mile High Distribution, avait constaté que ses œuvres étaient proposées sur des plateformes de téléchargement sans son autorisation. Elle avait alors mandaté une société allemande, Media Protector, pour collecter les adresses IP correspondant aux téléchargements illicites. 895 adresses IP ont ainsi été collectées entre fin 2017 et fin 2018.
Par une ordonnance sur requête, le TGI de Paris avait ordonné à la société Orange de conserver les fichiers permettant d'identifier les personnes ayant téléchargé ces œuvres. Dans un deuxième temps, la société Mile High Distribution a fait citer Orange en référé pour obtenir la communication des données d'identification. Cependant, Orange s'est opposée à la conservation et la communication de ces données.
Dans son jugement du 2 août 2019, le TGI de Paris a débouté la société Mile High Distribution au motif que la collecte avait été effectuée en violation de la loi Informatique et Libertés (version pré-RGPD) et du RGPD. Le tribunal a considéré que *« l'absence de caractère licite du traitement constitue un empêchement légitime à l'application des dispositions précitées de l'article 145 du code de procédure civile, sauf à porter une atteinte illégitime et disproportionnée aux droits et libertés fondamentales d'autrui, en l'espèce le droit à la protection des données à caractère personnel des individus dont les adresses IP ont été collectées ».* Le tribunal a notamment retenu que la société Mile High Distribution, en qualité de responsable du traitement établi en dehors de l'Union européenne, aurait dû i) désigner un représentant européen ; ii) tenir un registre des traitements identifiant le traitement des adresses IP, et iii) désigner un délégué à la protection des données (DPO) dans la mesure où elle collecte à grande échelle des données d'infraction.
(TGI Paris, ordonnance de référé du 2 août 2019, Mile High Distribution c. Orange)

Sécurité

Assurer la sécurité des données est l'une des principales obligations incombant aux responsables de traitements, comme précisé à l'article 32 du RGPD.
Plusieurs sociétés ont déjà été condamnées pour des atteintes à la sécurité des données et les sanctions continuent de tomber.

Sécurité des données – Sanction de 180.000 euros prononcée contre un site d'intermédiaire en assurance
La formation restreinte de la CNIL a prononcé une sanction de 180.000€ à l'encontre de la société Active Assurances pour manquement à son obligation de sécurité des données de ses utilisateurs.
Active Assurances exerce une activité d'intermédiaire en assurance et de distributeur de contrats d'assurance automobile aux particuliers. Elle édite un site web (activeassurances.fr) sur lequel les internautes peuvent demander des devis, souscrire des contrats, etc.
En juin 2018, la CNIL a été informée par un client qu'il était possible d'accéder aux données d'autres clients à partir de son compte personnel. La CNIL a alors réalisé un contrôle en ligne et a pu accéder aux copies de permis de conduire, cartes grises, RIB, etc. et alerté la société Active Assurances. Celle-ci a pris des mesures sans attendre. Cependant, lors d'un contrôle sur place, la CNIL a constaté que les mesures étaient insuffisantes (mots de passe de connexion correspondant à la date de naissance des clients, transmission de l'identifiant et du mot de passe de l'utilisateur par simple email). La formation restreinte a donc considéré que la société Active Assurances avait manqué à son obligation de sécurité. Compte tenu de la gravité du manquement (types de documents librement accessibles, nombre de personnes concernées, etc.) la CNIL a décidé de prononcer une amende de 180.000€ et de rendre la sanction publique.
(Délibération de la formation restreinte n° SAN – 2019-007 du 18 juillet 2019 prononçant une sanction pécuniaire à l'encontre de la société Active Assurances)

Union européenne

Royaume-Uni

Défaut de sécurité – British Airways risque une amende de 200 millions d'euros
Suite à une fuite massive de données (données personnelles, y compris bancaires) ayant concerné près de 500.000 clients en septembre 2018, l'autorité de contrôle britannique (Information Commissioner's Office – ICO) a déclaré qu'elle imposerait une amende de 183 millions de livres, correspondant à 1,5% des revenus de la compagnie aérienne pour 2017.
Les données personnelles de clients de British Airways avaient été collectées via un site frauduleux (phishing). Ce site aurait été actif entre les mois de juin et septembre 2018. Toutefois, la décision finale de l'ICO n'a pas encore été publiée.
("Intention to fine British Airways £183.39m under GDPR for data breach", ICO, 8 juillet 2019)

Espagne

Cookies – Publication d'un guide sur les cookies par l'AEPD (autorité de contrôle espagnole)

Comme la CNIL, et dans la mesure où les professionnels restent dans l'attente de lignes directrices claires sur l'utilisation des cookies, l'AEPD (autorité de contrôle espagnole) vient de publier des recommandations sur l'utilisation des cookies. Seuls les cookies nécessaires pour le fonctionnement d'un service web et les cookies techniques ne sont pas concernés par ces règles. Pour les autres cookies, les informations suivantes doivent être communiquées par l'éditeur du site : identifier la personne ayant placé les cookies (éditeurs du site ou tiers), objet du cookie, durée de conservation des données. Les conditions relatives aux cookies doivent être rédigées en termes clairs, dans un soucis de transparence. Enfin, on notera que pour l'AEPD, le fait de poursuivre la navigation sur le site entraîne l'acceptation des cookies.
(La AEPD presenta junto a la industria una guía sobre el uso de cookies adaptada a la nueva normativa, AEPD, 8 novembre 2019)

International

Amérique

Etats-Unis – Amende de 170 millions de dollars contre Google pour collecte illicite de données de mineurs

Le 4 septembre 2019, la Federal Trade Commission (FTC) a prononcé une amende de 170 millions de dollars à l'encontre de Google pour violation de la réglementation sur les données personnelles des enfants via sa filiale YouTube. Selon la FTC, YouTube collectait des données de mineurs en violation de la loi COPPA (loi américaine relative à la protection des données personnelles des mineurs de moins de 13 ans), afin de leur diffuser des publicités ciblées.

Cette amende a été prononcée suite à la conclusion d'un protocole d'accord entre Google, la FTC et le Ministère de la justice. Selon les autorités, YouTube collectait des données personnelles de mineurs (code d'identification pour suivre les vidéos regardées) sans l'accord des parents.

En vertu de l'accord, YouTube a également accepté de mettre en œuvre un système par lequel les ayant droits postant des vidéos devraient identifier si celles-ci sont destinées aux enfants, afin d'éviter la diffusion de publicités ciblées. Par ailleurs, YouTube doit obtenir le consentement des parents avant de collecter des données, telles que le nom d'un enfant ou ses photos.

Ces nouvelles règles de mise en ligne des vidéos et de recueil du consentement devraient être effectives début 2020.

("Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law", Federal Trade Commission, 4 septembre 2019)

Etats-Unis – Amende de 5 milliards de dollars prononcée à l'encontre de Facebook

Les amendes record continuent de tomber aux Etats-Unis à l'encontre des géants de l'internet.

Le 24 juillet 2019, la Federal Trade Commission (FTC) a prononcé une amende de 5 milliards de dollars à l'encontre de la société Facebook ! Le montant et les points devant être mis en conformité ont été détaillés dans un protocole d'accord conclu entre Facebook et la FTC. Cette amende sanctionne l'absence de mise en conformité de Facebook suite à un précédent protocole datant de 2012.

En vertu de ce protocole, Facebook doit se soumettre à un programme de surveillance pendant 20 ans. En outre, Facebook est tenu de mettre en place un comité indépendant de protection de la vie privée, nommé par le conseil d'administration de la société. Les membres de ce comité ne pourront être révoqués que par une super-majorité du conseil, afin d'éviter que Mark Zuckerberg exerce seul le contrôle sur ce comité.

Facebook devra également nommer des agents en charge de la conformité de la protection de la vie privée, approuvés par le comité de protection de la vie privée. Ces personnes devront vérifier la bonne application des points couverts par le protocole. Des attestations trimestrielles seront envoyées à la FTC.

La mise en conformité concerne les points suivants :

- La fourniture d'une information claire et visible par Facebook relative à l'utilisation de la reconnaissance faciale et le recueillement du consentement explicite des utilisateurs avant toute utilisation « qui sort de manière importante du cade d'usage tel qu'il a été présenté au préalable aux utilisateurs » ;
- L'interdiction d'utiliser les numéros de téléphone des utilisateurs, collectés pour activer une authentification sécurisée, à des fins publicitaires ;
- L'obligation de crypter les mots de passe des utilisateurs et de procéder à des audits réguliers pour détecter si ces mots de passe sont stockés en clair ; et
- L'amélioration de la surveillance des applications mobiles tierces, notamment les applications de développeurs qui omettent de certifier que celles-ci sont conformes aux politiques de Facebook ou de justifier leurs besoins spécifiques relatifs aux données des utilisateurs.

(« Facebook condamné à 5 Md $ par la FTC : et après ? », in Le Monde Informatique, 25 juillet 2019)

Asie

Chine – Entrée en vigueur de la nouvelle réglementation sur la protection des données personnelles des enfants

Le 23 août 2019, l'Administration du cyberespace chinoise a publié les « Mesures de protection des données personnelles des enfants en ligne ». Ces mesures, qui sont entrées en vigueur le 1er octobre dernier, viennent compléter la loi chinoise sur la cybersécurité. Ces mesures s'appliquent à toute

collecte, stockage, traitement, transfert et partage de données personnelles d'enfants de moins de 14 ans qui utilisent internet en Chine. Les mesures ne précisent pas si les sites web concernés sont limités à ceux qui s'adressent spécifiquement aux enfants, ni sur le fait que l'exploitant du site doit avoir connaissance du fait que des données d'enfants sont collectées. Apparemment, les sites web étrangers accessibles en Chine seraient également concernés par ces mesures.
Les mesures imposent qu'une notice d'information soit adressée aux parents ainsi qu'aux enfants. Les données ne peuvent être conservées que pendant une durée déterminée. Toutefois, le droit à la suppression des données ne peut être utilisé que dans deux cas : lorsque l'éditeur du site est en violation de la loi, ou s'il a violé les conditions d'utilisation du site.
Enfin, les mesures imposent la nomination par les éditeurs des sites web concernés, d'une personne dédiée à la protection des données des enfants.
(« China has released its version of COPPA", in The Privacy Advisor, 1er octobre 2019)

Publications

Retrouvez sur le Blog du Cabinet toutes nos dernières publications

Directeur de la publication : Bénédicte DELEPORTE
Editeur : DELEPORTE WENTZ AVOCAT - 5, rue Tronchet – 75008 Paris - Tel 01.40.17.95.86