LA LETTRE DU CABINET

DONNEES PERSONNELLES

Edito

Nous avons le plaisir de vous adresser le quatrième 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. Compte tenu de l'actualité sanitaire, nous reprenons également plusieurs informations en relation avec le Covid-19 et les traitements de données personnelles.

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

ⓘ Flash info – RGPD an 2 : la difficulté des entreprises à être en conformité au RGPD

Réglementation (p.2-4)
- Covid-19 : avis de la CNIL relatif à la mise en œuvre de l'application StopCovid ; Rappel des conditions de collecte de données de santé par les employeurs ; Report de la recommandation de la CNIL sur les cookies et autres traceurs
- Le CEPD rappelle les principes du consentement selon le RGPD
- La CNIL fait un point sur les techniques d'anonymisation des données

Conformité au RGPD/GDPR (p.4-7)
Actions des Autorités (CNIL, CEPD)
- Rappel sur l'obligation de contractualisation de la sous-traitance de données personnelles
- La CNIL communique sur les règles de réutilisation des données publiquement accessibles
- La CNIL publie un référentiel relatif à la gestion des ressources humaines
- Lancement d'une enquête sur les droits numériques des mineurs
- Publication du rapport 2019 du CEPD
- La CNIL communique sa stratégie de contrôle pour 2020

Enquêtes et mises en demeure
- Plusieurs enquêtes en cours en Europe contre des acteurs de la publicité en ligne

Jurisprudence
- Le Conseil d'Etat précise la portée géographique du droit au déréférencement
- La procédure de reconnaissance faciale à l'entrée de lycées invalidée par le tribunal administratif

International (p.8)
Asie
- Singapour : les obligations des employeurs en matière de protection des données de leurs salariés

ⓘ Flash info – RGPD an 2 : la difficulté des entreprises à être en conformité au RGPD

Deux ans déjà ! Le RGPD est entré en application le 25 mai 2018, mais il en ressort que de nombreuses entreprises tardent encore à se mettre en conformité. Et la crise sanitaire du Covid-19 a encore ralenti le mouvement…

Une étude menée par la société Tanium, réalisée auprès de 750 responsables informatiques au 1er trimestre 2020, révèle un décalage entre les investissements réalisés par les entreprises pour leur mise en conformité au RGPD et les résultats obtenus. 91% des entreprises consultées présentent des faiblesses informatiques qui les rendent vulnérables et potentiellement non conformes.

L'un des problèmes majeurs des entreprises tient à fragmentation des données (mass data fragmentation). Les entreprises manquent de visibilité globale sur leurs infrastructures physiques, virtuelles et cloud, et de contrôle de leurs actifs numériques. Plusieurs causes sont à l'origine de ce manque de visibilité, à savoir :

- Le manque de collaboration entre les équipes de sécurité et de production ;
- Le manque de moyens pour gérer efficacement le parc informatique ;
- Des systèmes trop anciens qui ne donnent pas les bonnes informations ;
- Des services qui installent leurs propres outils informatiques sans en informer la DSI ;
- L'installation d'un trop grand nombre de solutions dans l'entreprise ;
- Enfin, la généralisation du télétravail et de l'utilisation des appareils personnels des collaborateurs amplifient le problème de visibilité d'ensemble.

Une grande partie des données de l'entreprise repose notamment dans des bases de sauvegardes, des bases d'archivage, des environnements de développement ou de tests, ces différentes bases étant organisées le plus souvent en silos. En outre, les mêmes données peuvent être redondantes dans plusieurs outils ou sur plusieurs plateformes cloud. Il est donc très difficile de connaître avec précision quels traitements de données sont mis en œuvre dans l'entreprise, quelles catégories de données personnelles sont collectées et traitées, si ces données sont régulièrement supprimées, etc.

Outre la question de la conformité au RGPD, ces problèmes de visibilité sur les traitements de données personnelles créent des fragilités en termes de sécurité des données.

Quelques conseils pour améliorer la conformité au RGPD :

- Consolider le stockage secondaire (bases de sauvegarde, dossiers numériques, copies de développement, données d'analyse, etc.) sur une plateforme unique afin notamment d'éviter de recopier plusieurs fois les mêmes bases ;
- Sécuriser les données contre les accès non-autorisés, notamment par la pseudonymisation et s'assurer que seules les personnes autorisées ont accès à ces données ;
- Protéger les données contre leur perte et contre les rançongiciels (ransomware) ;
- Automatiser les sessions de suppression de données ;
- Utiliser des outils de recherche efficaces pour récupérer les données personnelles dans les différentes bases.

Enfin, on notera que le montant global des amendes prononcées en Europe depuis 2018 atteint 114 millions d'euros, alors que près de 161.000 notifications de violations de données ont été notifiées aux autorités de contrôle.

(« Etude Tanium : deux ans après le RGPD, les entreprises ne sont toujours pas conformes à la réglementation », in Global Security Mag, Avril 2020 et « GDPR 2 years in : achieving GDPR compliance 2 years on » in PrivSec.Report, 15 mai 2020)

Réglementation

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

Covid-19 – Avis de la CNIL relatif à la mise en œuvre de l'application StopCovid

Le 25 mai 2020, la Commission nationale de l'informatique et des libertés a rendu un avis sur le projet de décret relatif à l'application mobile StopCovid. Cet avis fait suite à un premier avis rendu le 24 avril sur le principe de mise en œuvre de l'application. Cette application, mise à disposition par le Gouvernement, fonctionne via Bluetooth. Elle a pour objet d'alerter les utilisateurs d'un risque de contamination au virus s'ils ont croisé des personnes infectées, elles-mêmes utilisatrices de l'application (système de suivi de contacts).

Dans la mesure où l'application a vocation à collecter des données personnelles de santé, la CNIL a été saisie pour avis.

L'application, dont le téléchargement sera volontaire, utilisera des données pseudonymisées, sans recours à la géolocalisation. Il n'y aura pas de création de fichier de personnes contaminées, mais uniquement une liste de contacts dont les données seront pseudonymisées. Par ailleurs, aucune conséquence juridique négative ne peut être appliquée aux personnes ne souhaitant pas utiliser l'application. Bien que réservée sur cette application, la CNIL a formulé des recommandations complémentaires, dont l'amélioration de l'information fournie aux utilisateurs, une information spécifique pour les mineurs et leurs parents, la confirmation d'un droit d'opposition et d'un droit à l'effacement des données et le libre accès aux codes sources.
L'application StopCovid a été mise à disposition du public début juin.
(CNIL : Délibération n°2020-056 du 25 mai 2020 portant avis sur un projet de décret relatif à l'application mobile dénommée « StopCovid »)

Covid-19 – La CNIL rappelle les conditions de collecte de données de santé par les employeurs
Le 7 mai dernier, la CNIL a rappelé aux employeurs les règles applicables à la collecte de données de santé dans le contexte du déconfinement et du retour des salariés sur leurs lieux de travail.
En principe, les données de santé sont interdites de traitement, sauf dans le cadre des exceptions prévues au RGPD (conditions de sécurité et de confidentialité renforcées, et traitement par les personnes habilitées uniquement). Les employeurs souhaitant mettre en place des procédures visant à s'assurer de l'état de santé de leurs employés doivent se conformer au droit du travail.

- *L'obligation de sécurité des employeurs*

Les employeurs sont soumis à une obligation de sécurité de leurs employés (art. L.4121-1 et R.4422-1 code du travail). Ils doivent notamment mettre en œuvre des actions de prévention des risques professionnels, mais également informer et former les salariés. Enfin l'organisation et les conditions de travail doivent être adaptés.
L'employeur peut rappeler à ses employés travaillant au contact d'autres personnes, de remonter toute information en cas de contamination éventuelle ou avérée, auprès de lui ou des autorités sanitaires compétentes pour adapter les conditions de travail, faciliter la transmission de ces informations par la mise en place de canaux dédiés et sécurisés, favoriser les modes de travail à distance et encourager le recours à la médecine du travail.

- *L'obligation de sécurité des employés*

En application de l'article L.4122-1 du code du travail, chaque employé doit veiller à préserver sa propre santé et sécurité, ainsi que celles des personnes avec qui il peut être en contact à l'occasion de son activité professionnelle. Pendant la pandémie, tout employé en contact avec des tiers (collègues ou public) doit informer l'employeur en cas de contamination avérée ou éventuelle. Par contre , les employés en télétravail qui seraient contaminés ne sont pas tenus d'informer leur employeur. L'arrêt de travail n'aura pas à mentionner la cause.
L'identité de la/des personne(s) infectée(s) ne doit pas être communiquée aux autres employés. Seules les données de date, d'identité de la personne, de contamination suspecte ou avérée, et de mesures organisationnelles prises peuvent être traitées par l'employeur.

- *Les différentes pratiques pendant la crise sanitaire*

Vérification de la température des salariés et clients : Les employeurs ne peuvent constituer des fichiers conservant les données de température des salariés. De même, il est interdit de déployer des outils de captation automatique de température. En revanche, l'utilisation d'un thermomètre manuel (type infrarouge sans contact), sans conservation des résultats, ni autre traitement, est autorisée.
Tests sérologiques et questionnaires de santé : selon la Direction générale du travail, les campagnes de dépistage organisées par les entreprises pour leurs salariés ne sont pas autorisées. Seuls les personnels de santé compétents, soumis au secret médical, peuvent collecter ces données.
(CNIL, « Coronavirus(Covid-19) : les rappels de la CNIL sur la collecte de données personnelles par les employeurs »)

Covid-19 – Report de la recommandation de la CNIL relative aux cookies et autres traceurs
Après avoir publié, en juillet 2019, des lignes directrices relatives aux cookies et autres traceurs, la CNIL a présenté le 14 janvier 2020 un projet de recommandation sur le recueil du consentement préalable des personnes à l'utilisation des cookies et traceurs. La publication de cette recommandation était prévue pour début avril 2020. Cependant, la crise sanitaire et son impact sur le marché publicitaire ont amenés la CNIL à annoncer le report de l'adoption de la version définitive de la recommandation à une date ultérieure, non encore précisée.
(site de la CNIL)

RGPD – Le CEPD rappelle les principes du consentement selon le RGPD
La notion de « consentement » a sensiblement évolué avec le RGPD, avec l'objectif de donner plus de maîtrise aux personnes concernées par la collecte de leurs données notamment. Le consentement est défini à l'article 4 (11) du RGPD comme « *toute manifestation de volonté libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.* »
Le Comité européen de la protection des données (CEPD ou EDPB – remplaçant du G29), a adopté le 4 mai dernier, des lignes directrices relatives au consentement, l'objet de ce document étant de préciser cette notion, et notamment le caractère « libre, spécifique, éclairée et univoque » du consentement.
Le consentement doit être recueilli par une déclaration ou un acte positif clair (par exemple cocher une case – « opt in »). L'internaute doit pouvoir visiter le site web même en cas de refus des cookies (sauf ceux techniquement nécessaires à son fonctionnement), et l'information sur les traitements de données et les cookies doit être claire et facilement compréhensible.
On notera par ailleurs que les « cookie walls » (page ou pop-up imposant l'acceptation des cookies avant de pouvoir accéder à un site web) ne sont pas conformes au RGPD car le consentement n'est pas libre et le refus entraîne l'impossibilité de visiter le site. De même, le fait de faire défiler une page (« scroll ») n'est pas conforme car le consentement de l'internaute n'est pas un acte positif clair.
(« Guidelines 05.2020 on consent under regulation 2016/679 », (en anglais), CEPD 4 mai 2020. Ces lignes directrices sont une mise à jour par rapport aux lignes directrices du G29 du 10 avril 2018)

Anonymisation des données – La CNIL fait un point sur les différentes techniques
Dans une communication du 19 mai dernier, la CNIL a rappelé les différentes techniques d'anonymisation et leurs conséquence en termes de conformité au RGPD. Ces techniques avaient été publiées dans un avis du G29 du 10 avril 2014.
Anonymisation et pseudonymisation sont deux pratiques distinctes.
Le RGPD prévoit la pseudonymisation de données, mais ne comporte pas d'obligation générale d'anonymisation.
L'anonymisation permet d'exploiter des données sans porter atteinte à la vie privée des personnes, et de conserver ces données au-delà de la durée de conservation initiale. Les règles de protection des données ne s'appliquent plus puisque la réutilisation et la diffusion des données anonymisées n'impacte pas la vie privée des personnes concernées. La CNIL fournit plusieurs conseils pour « construire un processus d'anonymisation pertinent » et pour vérifier l'efficacité de l'anonymisation. Une procédure d'anonymisation efficace doit remplir trois critères. Elle ne doit pas permettre : l'individualisation de personnes dans un jeu de données, la corrélation entre des ensembles de données distinctes sur un individu, et l'inférence, à savoir déduire de nouvelles informations sur une personne ; le risque étant la possibilité de ré-identifier les personnes (réversibilité).
La pseudonymisation consiste à remplacer des données directement identifiantes (nom, prénom), par des données non directement identifiantes (numéro séquentiel par exemple).
Contrairement à l'anonymisation qui doit être irréversible, la pseudonymisation est réversible.
(« L'anonymisation de données personnelles », CNIL 19 mai 2020 ; Avis 05/2014 du groupe de travail « article 29 » du 10 avril 2014 sur les techniques d'anonymisation)

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

Actions des autorités (CNIL, CEPD)

Sous-traitance de données personnelles – Modèles et clauses contractuelles types
Le RGPD prévoit un renforcement des obligations des sous-traitants et de leur contrôle par le responsable du traitement, en imposant notamment un contrat écrit relatif aux traitements de données personnelles sous-traitées.
L'article 28 du RGPD dispose que ce document « *définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement ».* Pour accompagner les parties impliquées, des clauses contractuelles types (ou CCT) doivent être proposées et adoptées par le CEPD.

La CNIL a publié un modèle-type de clauses de sous-traitance en octobre 2017, ainsi qu'un guide du sous-traitant. Plus récemment, l'autorité de contrôle danoise (Datatilsynet) a soumis son modèle de contrat de sous-traitance de données au CEPD qui a adopté ces CCT, par un avis publié en décembre 2019.
Pour les responsables de traitement ne l'ayant pas encore fait, la mise en conformité au RGPD passe par un recensement des sous-traitants et la mise à jour des contrats pour intégrer ces obligations.
(Guide du sous-traitant, CNIL, sept. 2017 ; Exemple de clauses de sous-traitance, CNIL, 4 oct. 2017 ; Avis 14/2019 sur le projet de CCT présenté par l'autorité de contrôle du Danemark, CEPD)

Prospection commerciale – La CNIL communique sur les règles de réutilisation des données publiquement accessibles en ligne
La CNIL a rappelé les conditions de réutilisation, à des fins marketing, de données personnelles publiquement accessibles en ligne. Ces données, notamment téléphoniques, bien que publiquement accessibles, sont des données personnelles soumises à la réglementation sur la protection des données.
La CNIL a réalisé plusieurs contrôle courant 2019 auprès de sociétés récupérant des données en ligne grâce à des logiciels d'extraction (web scraping) par exemple. Même si cette pratique n'est pas expressément interdite, elle est soumise à la réglementation sur la protection des données.
La première obligation concerne le recueil du consentement des personnes concernées, avant même d'engager les actions de prospection, ainsi que le respect du droit d'opposition. La CNIL rappelle que « *l'acceptation par un internaute, de manière générale et indifférenciée, des conditions d'utilisation (CGU) d'un service ne peut être assimilée à un consentement spécifique, même si ces conditions d'utilisation informeraient l'internaute de son engagement à recevoir de la prospection commerciale par voie électronique*. »
Les points à contrôler avant d'utiliser un logiciel d'aspiration de données doivent porter sur :

- La vérification de la nature et de l'origine des données,
- La minimisation de la collecte de données,
- L'information des personnes concernées par la collecte
- L'encadrement contractuel de la prestation avec les sous-traitants, et si nécessaire
- La réalisation d'une analyse d'impact.

(« La réutilisation des données publiquement accessibles en ligne à des fins de démarchage commercial », CNIL, 30 avril 2020)

Ressources humaines – La CNIL publie un référentiel relatif à la gestion des ressources humaines
La CNIL vient d'adopter un référentiel relatif aux traitements de données aux fins de gestion des ressources humaines, en remplacement de la norme simplifiées NS-46. Ce référentiel concerne tous les employeurs, publics et privés pour les traitements de recrutement, de gestion administrative du personnel, de rémunération ou de mise à disposition d'outils de travail. Le référentiel précise notamment les cas dans lesquels la réalisation d'une analyse d'impact est obligatoire ou non.
Ce nouveau référentiel exclut toutefois plusieurs traitements concernant les salariés, tels que le contrôle d'accès aux locaux de l'entreprise via des dispositifs biométriques, le dispositif d'alerte professionnelle (objet d'un référentiel publié le 10 décembre 2019), la vidéosurveillance, etc.
(« Référentiel relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion du personnel », publié le 15 avril 2020)

Droits des mineurs – La CNIL lance une enquête sur les droits numériques des mineurs
Les droits numériques des mineurs sont couverts par l'article 8 du RGPD. La loi Informatique et Libertés fixe à 15 ans l'âge à partir duquel le mineur peut consentir seul au traitement de ses données personnelles, lorsque le traitement est effectué dans le cadre de services en ligne. En deçà de 15 ans, le consentement doit être donné conjointement par le mineur et un titulaire de l'autorité parentale. Toutefois, ni le RGPD, ni la loi Informatique et Libertés, ne définissent les conditions dans lesquelles un mineur peut accomplir seul certains actes sur internet, ni les modalités de vérification de l'âge du mineur et de recueil du consentement des parents et des enfants.
Le 21 avril, la CNIL a donc lancé une consultation publique pour recueillir l'avis des parties prenantes (professionnels du numérique, de l'enfance, associations collégienne et lycéennes, parents, etc.) sur les conditions dans lesquelles un mineur peut accomplir certains actes sur internet, tels que s'inscrire sur un réseau social, faire des achats en ligne, faire jouer ses droits d'accès, de rectification, d'effacement ou d'opposition.
(« Enquête sur les droits des mineurs dans l'environnement numérique », site de la CNIL)

CEPD – Publication du rapport annuel 2019

Le Comité européen de la protection des données (CEPD) a publié, courant mars 2020, son rapport annuel pour l'année 2019. Composé des 28 autorités de contrôle chargées de la protection des données, le CEPD est en charge de la cohésion de la mise en œuvre du RGPD au sein de l'Union européenne.

Pour le CEPD, l'année 2019 a été marquée par la mise en pratique des nouvelles règles fixées par le RGPD. Son activité porte notamment sur la fourniture d'orientations et de conseils pour les Etats membres de l'UE et sur la poursuite des efforts de convergence de la protection des données au niveau international.

Concernant les orientations et conseils, le CEPD a continué sa mission auprès des institutions européennes dans le domaine de la sécurité des frontières de l'UE, les politiques de l'UE en matière d'asile, de coopération policière et de migration. Plusieurs lignes directrices ont été publiées, dont les lignes directrices sur l'évaluation de la proportionnalité des traitements destinées aux responsables politiques, et les lignes directrices sur les rôles et notions de responsables du traitement, de sous-traitant et de responsabilité conjointe. Le CEPD a par ailleurs lancé la publication de TechDispatch, consacrant chaque numéro à une technologie différente et son évaluation sur le respect de la vie privée. Enfin, le CEPD a poursuivi ses travaux sur le développement du réseau d'ingéniérie de la vie privée sur internet (IPEN) rassemblant des experts de différents domaines pour encourager la mise en œuvre de solutions liées au respect de la vie privée.

Concernant l'action à l'international, l'IPEN a travaillé au développement de la convergence de la protection des données et encouragé un débat sur l'éthique numérique.

(Rapport annuel du CEPD, 2019. Une année de transition)

Conformité au RGPD – La CNIL communique sa stratégie de contrôle pour 2020

Comme chaque année, la CNIL a publié sa politique de contrôle pour l'année 2020. Cette politique de contrôles de conformité se focalise sur des domaines d'activité spécifiques, généralement à risque pour le respect de la vie privée. En plus des contrôles réalisés suite à des plaintes ou des thèmes révélés par les médias, cette année, la CNIL a décidé d'axer sa politique de contrôles sur trois thématiques :

- les données de santé, notamment via la télémédecine, les objets connectés et les violations de données ;
- la géolocalisation pour les services de proximité par les applications de recommandations de transport ou l'optimisation des déplacements par exemple ; et
- les cookies et autres traceurs, notamment utilisés pour le ciblage publicitaire et le profilage des utilisateurs.

(« Quelle stratégie de contrôle pour 2020, », CNIL 12 mars 2020)

Enquêtes et 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.

Publicité en ligne – Plusieurs enquêtes en cours en Europe

Depuis fin 2018, plusieurs enquêtes ont été ouvertes contre des acteurs de la publicité en ligne pour contrôler la conformité de leurs pratiques au RGPD. L'ONG britannique Privacy International a déposé plusieurs plaintes auprès des autorités de contrôle, en France (CNIL), en Irlande (DPC) et au Royaume-Uni (ICO). Selon Privacy International, « *l'écosystème de l'Adtech repose sur de vastes atteintes à la vie privée, exploitant les données des personnes au quotidien* ». En France, la CNIL a ouvert une enquête contre la société de reciblage publicitaire Criteo. L'autorité irlandaise enquête sur la société Quantcast (publicité en ligne). Quant au Royaume-Uni, l'enquête de l'ICO concerne le courtier de données Acxiom et les sociétés d'évaluation de risque (credit score) Experian et Equifax. Ces enquêtes portent notamment sur les conditions de recueil du consentement des internautes par ces acteurs de la publicité en ligne.

(« La CNIL ouvre une enquête sur Criteo pour violation du RGPD », in L'Usine Digitale, 10 mars 2020 ; « Données personnelles : le français Criteo visé par une enquête de la Cnil » in La Tribune, 11 mars 2020)

Jurisprudence

Déréférencement - Le Conseil d'Etat précise la portée géographique du droit au déréférencement
Le droit à l'oubli découle d'un arrêt de la Cour de justice de l'Union européenne (CJUE) de 2014. Pour rappel, le droit à l'oubli, ou droit au déréférencement permet à toute personne de demander à l'exploitant d'un moteur de recherche de supprimer certains résultats qui apparaissent suite à une requête faite sur ses nom et prénom.
En 2016, la CNIL avait prononcé une sanction pécuniaire de 100.000 euros à l'encontre de Google pour ne pas s'être conformé à une mise en demeure de la CNIL, lui enjoignant d'appliquer les mesures de déréférencement mondiales -à l'ensemble des version nationales de son moteur de recherche-, et non aux seules extensions européennes. Depuis mars 2016, Google avait toutefois mis en place un système de redirection automatique vers la version du site national de l'internaute, et le blocage du contenu déréférencé sur ce territoire. Selon Google, cette mesure de redirection était suffisante. Google a saisi le Conseil d'Etat pour contester la sanction de la CNIL.
Dans un arrêt du 27 mars 2020, le Conseil d'Etat, appliquant la décision de la CJUE rendue le 24 septembre 2019, annule la sanction de la CNIL et précise le périmètre territorial du déréférencement.
Le principe du déréférencement est ainsi limité au territoire de l'Union européenne. Il appartient au Conseil d'Etat d'apprécier le caractère effectif des mesures de déréférencement prises par le moteur de recherche. Il revient à l'autorité de contrôle (CNIL) ou au Conseil d'Etat d'obliger le déréférencement des résultats par le moteur de recherche au cas par cas.
Cette décision, rendue sous l'empire de la directive du 24 octobre 1995 sur la protection des données et sous l'ancienne version de la loi Informatique et Libertés, reste entièrement applicable avec le RGPD.
(CJUE, affaire C-131/12 du 13 mai 2014, Google Spain SL, Google Inc. c. AEPD, Mario Costeja Gonzalez ; CJUE, affaire C-507/17 du 24 sept. 2019, Google Spain LLC c. CNIL ; CE, décision du 27 mars 2020 n°399922, Google Inc.)

Données biométriques – La procédure de reconnaissance faciale à l'entrée de lycées invalidée
Dans une décision du 27 février 2020, le tribunal administratif de Marseille a annulé la délibération du conseil régional de la région Provence-Alpes-Côte d'Azur du 14 décembre 2018 ayant autorisé le lancement d'une expérimentation de contrôle d'accès par reconnaissance facial dans 2 lycées de Marseille et de Nice.
L'article 9 du RGPD, applicable aux traitements de données biométriques, dont les données de reconnaissance faciale dispose que *« 1. Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, (…), ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.*
2. Le paragraphe 1 ne s'applique pas si l'une des conditions suivantes est remplie : a) la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, (…); g) le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée (…) ».
Par sa délibération du 14 décembre 2018, la région PACA avait lancé une expérimentation de contrôle d'accès par reconnaissance faciale dans deux lycées. L'association la Quadrature du Net et la fédération de parents d'élèves FCPE notamment, ont engagé un recours pour excès de pouvoir contre la Région. Selon le tribunal administratif de Marseille, d'une part la région PACA n'a pas prévu de garanties suffisantes afin d'obtenir des lycéens et de leurs parents leur consentement libre et éclairé à la collecte de leurs données ; d'autre part, la région n'a pas recherché si les finalités de fluidification et de sécurisation des contrôles d'accès dans les lycées constituaient un motif d'intérêt public ou si elles ne pouvaient être atteintes par d'autres moyens moins intrusifs, tels que les badges ou la vidéosurveillance.
Enfin, le tribunal a jugé que la région n'était pas compétente pour adopter ce type de délibération, dans la mesure où les missions d'encadrement des élèves relèvent de la compétence des chefs d'établissement.
(TA Marseille, 9é ch., 27 février 2020, La Quadrature du Net et Autres)

International

Asie

Singapour – quelles obligations pour les employeurs en matière de protection des données de leurs salariés

La loi singapourienne sur la protection des données personnelles (Personal Data Protection Act 2012), entrée en application en juillet 2014, devrait être remaniée courant 2020. La loi s'applique à tout organisme ayant des activités à Singapour, quelle que soit sa taille. Bien que généralement moins stricte que le RGPD, la loi singapourienne de protection des données impose certaines obligations spécifiques.

Les traitements de données personnelles sont soumis au consentement de la personne concernée, y compris les salariés, sauf dans les cas suivants : le traitement est raisonnable pour gérer ou mettre un terme au contrat de travail ; le traitement est réalisé à des fins d'évaluation (embauche, promotion, licenciement) ; les données personnelles sont disponibles publiquement, par exemple, sur le profil LinkedIn du salarié ou sur un blog.

Les salariés doivent toutefois être informés de la finalités des traitements de leurs données.

D'autres dispositions sont spécifiques à la loi singapourienne, telles que les règles applicables à la collecte et le traitement des numéros d'identification des personnes (numéros de passeports et FIN – foreign identification numbers), l'obligation pour les employeurs de nommer au moins un délégué à la protection des données (DPO) à Singapour, les obligations relatives au transfert de données personnelles à l'international. A ce titre, on retiendra que Singapour est membre du système de Cross-Border Protection Rules (CBPR), accord applicable à certains pays de la zone Asie-Pacific. (1)

Enfin, les principes suivants s'appliquent aux traitements de données sous la loi singapourienne : les données doivent être exactes et complètes. Les employeurs sont soumis à une obligation de sécurité, administrative, technique et physique, des données. Les employés ont un droit d'accès et de rectification de leurs données, et la durée de conservation des données est limitée à la durée nécessaire au traitement.

En cas de violation de la loi, le montant maximum des sanctions financières s'élève à 1 million de S$ (environ 640.000€). Depuis l'entrée en application de la loi, la Commission sur la protection des données personnelles (Personal Data Protection Commission ou PDPC) a publié plus de 135 décisions, sachant que la pénalité la plus importante, 1 million de dollars, a été prononcée le 14 janvier 2020 dans l'affaire de la violation de données de santé de SingHealth, l'organisme public de santé de Singapour (1,5 millions de comptes de patients affectés).

Si votre société a des opérations à l'international, dont Singapour, et que vous avez adopté une politique globale de protection des données des salariés, celle-ci devra être adaptée en tant que de besoin au niveau local.

(1) Outre Singapour, les pays membres du système CBPR sont l'Australie, le Canada, la Corée, le Japon, le Mexique, Taiwan et les Etats-Unis.

(Personal Data Protection Act 2012, 20 nov. 2012; site de la PDPC, l'autorité de contrôle singapourienne : www.pdpc.gov.sg)

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