LA LETTRE DU CABINET

DONNÉES PERSONNELLES

EDITO

Nous avons le plaisir de vous adresser le second numéro de notre nouvelle 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 : un point flash sur le bilan après un an d'application du RGPD, 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

ⓘ FLASH – RGPD, UN AN APRÈS

Le règlement général sur la protection des données (RGPD), est entré en application il y a un an, le 25 mai 2018. Cette première année a vu l'intensification de la mise en conformité par les organismes (entreprises, associations, administrations) et, en parallèle, les premières sanctions post-RGPD prononcées par les autorités de contrôle, en France et dans plusieurs pays européens.
La CNIL a publié un bilan de lapplication du RGPD à l'occasion de ce premier anniversaire. Les points à retenir sont les suivants :
- Outre une prise de conscience des citoyens sur la problématique de la protection des données personnelles (70% des Français y seraient plus sensibles), la CNIL a constaté une augmentation de 30% du nombre de plaintes qui lui ont été adressées depuis un an. La Commission relève également le développement de la coopération entre les autorités de contrôle européennes avec 800 procédures initiées dans d'autres pays dans lesquelles elle est impliquée ;
- Les violations de données (failles de sécurité, hacking, etc.) doivent désormais être déclarées à la CNIL par toutes les organisations victimes. 2.044 notifications de violations de données ont été reçues par la CNIL, et 89.271 notifications de violations de données ont été relevées au niveau européen ;
- Plus de 19.000 délégués à la protection des données (DPO) ont été désignés.
En 2019, la CNIL passe à un « rythme de croisière ». Alors que la CNIL avait déclaré que la première année du RGPD serait consacrée à la mise en conformité, elle considère que la période de transition est terminée. L'instruction des plaintes et les contrôles seront réalisés au regard d'une pleine conformité au RGPD, sous réserve de la prise en compte de la gravité des manquements (notamment à l'obligation de sécurité), de la célérité des organismes à corriger les manquements identifiés et de leur coopération avec la CNIL, éléments justifiés pour alourdir ou alléger les sanctions en cas de violation du règlement.
L'action pédagogique de la CNIL est enfin rappelée avec la mise en ligne de guides pratiques (sensibilisation des collectivités locales, kit développeur – voir plus bas), la publication de référentiels, remplaçant les normes simplifiées pré-RGPD (gestion des RH, de la relation clients, de la gestion des impayés), des règlements-types et des outils pratiques d'aide à la conformité (liste des organismes ayant désigné un DPO, MOOC sur le RGPD, etc.).
(« Quelle stratégie de contrôle pour 2019 », 19 avril 2019 et « Un an de RGPD : une prise de conscience inédite », 23 mai 2019, site de la CNIL)

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

Informatique et Libertés – Entrée en vigueur de la nouvelle loi Informatique et Libertés et du dernier décret d'application pour mise en conformité au RGPD
La nouvelle réglementation sur la protection des données personnelles est désormais complète avec la publication du décret d'application du 29 mai 2019.
Le RGPD comprend une série de dispositions dont les modalités d'application devaient faire l'objet d'adaptation des lois nationales sur la protection des données. En France, cette adaptation a été faite en plusieurs étapes : la loi Informatique et Libertés a été profondément modifiée le 20 juin 2018 et a été complétée par un décret d'application du 1er août 2018. Elle a ensuite été réécrite et mise en cohérence avec l'ordonnance du 12 décembre 2018. Enfin un nouveau décret d'application de la loi en date du 29 mai 2019 vient d'entrer en vigueur.
Les principaux points de ce décret à retenir sont les suivants : la composition et le fonctionnement de la CNIL ; les modalités de contrôle de la mise en œuvre des traitements ; la CNIL en tant qu'autorité chef de file ; les formalités préalables à la mise en œuvre des traitements (notamment demandes d'avis et d'autorisation) ; les règles relatives aux codes de conduite, BCR et certificats ; et des précisions complémentaires sur la mise en œuvre de la règlementation (droits de la personne

concernée, obligations incombant au responsable du traitement et au sous-traitant, traitements de données personnelles dans le domaine de la santé, etc. ; ainsi que des modalités quant à la mise en œuvre de la directive « police-justice ».
(Décret n°2019-536 du 29 mai 2019 pris pour l'application de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)

Marketing en ligne – La CNIL publie une recommandation sur la transmission de données à des partenaires commerciaux
Le 28 décembre 2018, la CNIL a publié une recommandation sur la transmission de données à des partenaires commerciaux, venant compléter sa recommandation sur la prospection commerciale par courrier électronique. Les règles relatives à la prospection commerciale par courrier électronique ne sont pas modifiées depuis l'entrée en application du RGPD. En revanche, la CNIL précise les règles relatives à la transmission de données aux partenaires commerciaux des organismes ayant procédé à la collecte initiale (sites commerciaux ou courtiers de données) dans le respect du RGPD.
Cette activité est soumise à trois séries d'exigences, sur la bases des principes de consentement et d'information de la personne concernée. Il faut désormais deux niveaux de consentement et deux niveaux d'information :

1) Le consentement de la personne concernée doit être recueilli par la société qui collecte les données personnelles, avant toute transmission de ces données. En pratique, les sociétés qui collectent des données personnelles prévoient 2 cases à cocher sur le formulaire de collecte, une case autorisant le traitement des données par la société elle-même, et une case autorisant le partage des données avec les « partenaires commerciaux » de la société.

2) Le consentement recueilli par la société qui collecte les données pour partage avec ses partenaires commerciaux n'est valable que pour ces derniers. Les partenaires ne peuvent par la suite transmettre les données personnelles reçues à leurs propres partenaires sans avoir demandé à nouveau le consentement des personnes concernées. Les courtiers de données, qui transmettaient des bases de données « opt in » sont donc directement impactés puisqu'ils devront redemander le consentement des personnes concernées avant tout nouveau transfert.

3) Les partenaires commerciaux à qui les données sont transférées doivent être identifiés. La liste des partenaires peut figurer soit sur le formulaire de collecte, soit sur un document séparé, accessible par un lien hypertexte depuis le formulaire, cette deuxième option étant plus aisée en cas de mises à jour régulières. La CNIL recommande par ailleurs d'ajouter un lien vers les politiques sur la protection des données desdits partenaires commerciaux.

Les personnes doivent enfin être informées de l'évolution de la liste des partenaires. Les messages envoyés par la société à l'origine de la collecte doivent permettre de prendre connaissance de la liste à jour des partenaires et la première communication d'un nouveau partenaire doit informer la personne, au plus tard dans un délai d'un mois, du traitement qu'il fait de ses données.
Le droit d'opposition de la personne peut être exercé par la personne concernée soit directement auprès du nouveau partenaire, soit auprès de la société à l'origine de la collecte initiale qui devra le répercuter à ses partenaires.
Ainsi, on retiendra que le consentement de la personne concernée et son information sont désormais requis non seulement lors de la première collecte de données, mais également après chaque transfert à un nouveau partenaire. Ces exigences doivent être mises en œuvre dans les formulaires de collecte ainsi que dans les documents contractuels entre les partenaires commerciaux.
(Recommandations « La prospection commerciale par courrier électronique » et « Transmission des données à des partenaires à des fins de prospection électronique : quels sont les principes à respecter ? », 28 décembre 2018, Site de la CNIL)

Biométrie – La CNIL publie un règlement-type sur la biométrie sur les lieux de travail
Le 10 janvier 2019, la CNIL a publié un règlement-type sur la biométrie sur les lieux de travail. Ce document a pour objet de préciser les obligations applicables aux employeurs qui souhaitent mettre en place un dispositif biométrique de contrôle d'accès aux locaux, et aux outils numériques.
Pour rappel, selon l'article 9 du RGPD, les données biométriques sont qualifiées de données sensibles. L'article 8 de la loi Informatique et Libertés modifiée interdit les traitements de données biométriques. Cette interdiction de principe peut être levée sous réserve que le dispositif de contrôle d'accès biométrique soit conforme au règlement type de la CNIL. Il est à noter que ce règlement est contraignant.
(Délibération n°2019-001 du 10 janvier 2019 portant sur le règlement type relatif à la mise en oeuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques)

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)

CNIL – Présentation du rapport d'activité 2018
La CNIL a publié son rapport d'activité 2018 le 15 avril dernier. Il s'agit de son premier rapport annuel après l'entrée en application du RGPD, le règlement ayant fortement impacté l'activité de la Commission.
Le bilan 2018 s'articule autour de trois axes :

1) L'accroissement du nombre de plaintes et des notifications de violations de données, et l'apparition de nouvelles tendances : le nombre des plaintes reçues par rapport à l'année précédente est en hausse de 30%. Celles-ci se répartissent entre les domaines suivants : internet (problèmes de suppression de données personnelles notamment) (35,7%), marketing/commerce (21%), RH (16,5%), banque et crédit (8,9%) et santé et social (4,2%).
Des tendances apparaissent, notamment les demandes de portabilité des données des clients des banques et des services de contenus en ligne, une plus grande sensibilité des personnes à la sécurité de leurs données personnelles et la crainte des utilisateurs de smartphones concernant l'accès des applications mobiles à leurs données personnelles.

2) La poursuite de l'activité pédagogique avec la mise en ligne de nouveaux outils pour accompagner la mise en conformité au RGPD : publication de guides, référentiels, MOOC RGPD, etc.

3) L'activité répressive avec 310 contrôles réalisés en 2018. La CNIL indique que dans la majorité des cas, « *la simple intervention de la CNIL se traduit par une mise en conformité de l'organisme*. » 40 mises en demeure ont néanmoins été adoptées et 11 sanctions prononcées par la formation restreinte (organe de la CNIL en charge de prononcer les sanctions).
En 2019, la CNIL affiche deux axes d'intervention : la pédagogie notamment avec la poursuite de la publication d'outils d'aide à la mise en conformité et la publication d'un guide sur l'open data, et la dissuasion avec un programme de contrôle portant plus particulièrement sur la répartition des responsabilités entre les sous-traitants et les responsables de traitement, et les traitements de données des mineurs.
(Rapport d'activité 2018, 15 avril 2019, Site de la CNIL)

Coopération – Poursuite du programme de coopération entre la CNIL et la DGCCRF
La CNIL et la DGCCRF ont développé un programme de coopération depuis 2011. Un nouveau protocole de coopération a été conclu entre les deux organismes le 31 janvier 2019, mettant notamment l'accent sur la sensibilisation des consommateurs sur les risques encourus lors de la communication de leurs données personnelles ; un échange d'informations facilité entre les deux organismes concernant le non-respect de droit de la consommation et de la protection des données ; l'organisation de contrôles communs ; et la mutualisation des expertises (outils d'enquête).
Cette coopération fera l'objet de bilans annuels de suivi.
(Communication du 31 janvier 2019, Site de la CNIL)

MISES EN DEMEURE POUR NON-CONFORMITÉ

Une procédure de mise en demeure n'entraîne pas obligatoirement une sanction de la CNIL. Deux séries de procédures de mises en demeure ouvertes courant 2018 viennent d'être clôturées par la CNIL après qu'elle ait constaté que les sociétés en cause s'étaient mises en conformité.

Détournement de finalité du traitement – Clôture des mises en demeure contre cinq sociétés d'assurance
Le 25 septembre 2018, la présidente de la CNIL avait mis en demeure cinq société des groupes Humanis et Malakoff-Médéric pour détournement de la finalité des traitements des assurés (voir notre précédente Newsletter). Lors d'un contrôle, la CNIL avait relevé que ces sociétés utilisaient les données personnelles de leurs assurés à des fins de prospection commerciale alors que le traitement avait pour finalité la mise en œuvre des régimes de retraite complémentaire. Plusieurs dizaines de milliers de personnes étaient concernées. Les sociétés s'étant mises en conformité (modification du système informatique, suppression des données acquises illégalement, formation interne à la

protection des données personnelles), les procédures de mises en demeure ont été clôturées le 21 février 2019.
(Communication de la CNIL sur la clôture des mises en demeure à l'encontre des sociétés des groupes Humanis et Malakoff-Médéric, Site de la CNIL)

Absence de consentement des personnes concernées - Clôture de la mise en demeure à l'encontre de la société Vectaury
Le 8 novembre 2018, la présidente de la CNIL avait mis en demeure la société Vectaury pour absence de recueil du consentement des utilisateurs au traitement de leurs données de géolocalisation à des fins de ciblage publicitaire (voir notre précédente Newsletter). Les données provenaient des applications mobiles exploitées par des sociétés partenaires de Vectaury et des offres d'enchères d'espaces publicitaires sur des applications mobiles, reçues par Vectaury. Suite à cette mise en demeure, la société Vectaury s'étant mise en conformité (affichage d'une bannière informative lors de l'installation des applications mobiles pour recueillir le consentement des utilisateurs et collecte des données des utilisateurs ayant donné leur consentement à l'organisme collecteur des données pour le service d'enchères d'espaces publicitaires), la procédure de mise en demeure a été clôturée le 26 février 2019.
(Communication de la CNIL sur la clôture de la mise en demeure à l'encontre de la société Vectaury, Site de la CNIL)

JURISPRUDENCE

Traitement de données – Un gendarme sanctionné pour détournement de finalité
Dans une décision du 24 avril 2019, le Conseil d'Etat a confirmé la sanction prononcée par le ministère de la Défense (15 jours d'arrêt) en avril 2016 contre un gendarme qui avait consulté des fichiers de gendarmerie à des fins personnelles pour rechercher des informations sur l'employeur de sa fille et sur d'autres personnes. Une telle consultation constitue un détournement de la finalité du traitement de données personnelles.
Aux termes de l'article 230-10 al.1 du code de procédure pénale (rédaction antérieure à l'ordonnance n°2018-1125 du 12 décembre 2018), « *Les personnels spécialement habilités des services de la police et de la gendarmerie nationales (…), peuvent accéder aux informations, y compris nominatives, figurant dans les traitements de données personnelles prévus par la présente section et détenus par chacun de ces services. L'habilitation précise la nature des données auxquelles elle autorise l'accès (…)* ». Le fait de détourner ces informations de leur finalité est puni d'une peine maximum de cinq ans d'emprisonnement et de 300 000 euros d'amende. La Cour en a déduit qu'un gendarme qui consulte à des fins personnelles des traitements comportant des données à caractère personnel commet un manquement à ses obligations, à savoir un détournement de la finalité du traitement. Cette faute, de nature à justifier une sanction disciplinaire, est considérée comme étant proportionnée en l'espèce compte tenu des faits et du caractère répété et persistant des manquements (les consultations ont été réalisées sur une période d'une année).
(Conseil d'Etat, 7é ch., 24 avril 2019)

Géolocalisation – Cassation d'un arrêt validant un système de géolocalisation des salariés
Dans un arrêt rendu le 19 décembre 2018, la Cour de cassation a cassé la décision de la Cour d'appel de Lyon du 13 janvier 2017 qui avait validé le système de géolocalisation de postiers.
En l'espèce, la société Mediapost, filiale du groupe La Poste en charge de la distribution des publicités, avait mis en place un système de géolocalisation de ses personnels - un boîtier activé par l'employé enregistrait sa localisation toutes les 10 secondes. La fédération Sud PTT considérait ce système illicite et a assigné la société Mediapost. La Cour rappelle que, selon l'article L.1121-1 du code du travail, « *Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché*. » En conséquence, selon la Cour, 1) un système de contrôle de la localisation des salariés n'est licite que si le contrôle ne peut être opéré par un autre moyen de contrôle de la durée du travail, fût-il moins efficace que la géolocalisation, et 2) ce système ne peut être justifié lorsque le salarié dispose d'une liberté dans l'organisation du travail. Or, la Cour d'appel n'a pas recherché si le système de géolocalisation mis en place était le seul moyen de contrôler la durée du travail des salariés. En conséquence, la cour de cassation a cassé et annulé l'arrêt d'appel.
(Cass. soc., 19 décembre 2018, Fédération Sud PTT/ Mediapost)

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. Dans cette rubrique, nous traitons les questions liées à la sécurité des données, notamment à travers les dernières décisions publiées.

Security et privacy by design - La CNIL publie un kit de bonnes pratiques à destination des développeurs
Dans le cadre de la mise en oeuvre des principes de sécurité et de protection des données dès la conception (« security » et « privacy by design »), la CNIL a publié un kit de bonnes pratiques destiné aux développeurs. Ce kit est organisé en quatre parties, chacune étant accompagnée de conseils :

1) Choisir ses outils de travail, en se posant des questions, relatives notamment à la sécurité ;

2) Préparer son développement, en mettant en œuvre le principe de sécurité dès la conception ; une méthodologie de la sécurité est d'ailleurs proposée ;

3) Adopter les bonnes pratiques pour gérer son code source, en pensant à l'architecture de l'outil de gestion (Git, Mercurial, Github, Gitlab, etc.), gérer les paramètres de visibilité des dépôts de code, gérer les permissions d'accès et de « commit », etc. ;

4) Comment intégrer les bibliothèques, SDK ou outils tiers dans les applications ? Utiliser des systèmes de gestion de dépendances, changer les configurations par défaut, auditer les bibliothèques et SDK, etc.

L'objectif de ce kit développeur est de mettre à leur disposition une série de conseils pour les sensibiliser à la protection des données et mettre en œuvre les principes de sécurité et de protection des données dès la conception.
(« Développeurs : la CNIL met en ligne un kit de bonnes pratiques », 13 mai 2019, Site de la CNIL)

Défaut de sécurité – Sanction de 400.000 euros contre une agence immobilière pour atteinte à la sécurité des données et non-respect des durées de conservation
Le 28 mai 2019, la formation restreinte de la CNIL a prononcé une sanction pécuniaire de 400.000€ à l'encontre de la société Sergic, une agence immobilière, pour manquement à ses obligations de sécurité et de limitation de la durée de conservation des données.
La CNIL a réalisé un contrôle en ligne à la suite de la plainte d'un utilisateur qui avait pu avoir accès, depuis son espace personnel sur le site de l'agence, à des documents d'autres utilisateurs (copies de cartes d'identité, cartes Vitale, avis d'imposition, etc.). Le contrôle a révélé deux manquements :

- une atteinte à l'obligation de sécurité (article 32 du RGPD), la société ayant omis de mettre en place une procédure d'authentification des utilisateurs du site. Deux circonstances aggravantes ont été retenues : la nature des données rendues accessibles, et le fait que la société avait connaissance de la vulnérabilité depuis 6 mois et n'avait pris aucune mesure pour en limiter l'impact en attendant la correction définitive ; et
- un manquement à la limitation de la durée de conservation des données, les documents des utilisateurs étant conservés sans limitation de durée.

Le montant de la sanction prend en compte la gravité du manquement, le manque de diligence de la société pour corriger la vulnérabilité et la nature des documents accessibles.
(Délibération de la formation restreinte n° SAN – 2019-005 du 28 mai 2019 prononçant une sanction pécuniaire à l'encontre de la société SERGIC)

Défaut de sécurité – Le Conseil d'Etat confirme la procédure de sanction de la CNIL et sa proportionnalité
En juin 2017, lors d'un contrôle en ligne sur les traitements mis en œuvre par l'Association pour le développement des foyers (ADEF), la CNIL a constaté un défaut de sécurité permettant à des tiers non autorisés d'accéder aux données personnelles des personnes sollicitant les services de l'association. L'association n'a réagi, fin juin 2017, qu'après plusieurs demandes de correction des défauts de sécurité par la CNIL. Le 21 juin 2018, la formation restreinte de la CNIL a prononcé une sanction pécuniaire de 75.000€ et décidé de rendre la sanction publique pendant 2 ans. Considérant cette sanction disproportionnée, l'ADEF a demandé l'annulation de la délibération.
Dans sa décision du 17 avril 2019, le Conseil d'Etat confirme deux points :
1) Concernant la procédure de sanction, les juges considèrent que « *la formation restreinte de la CNIL peut, sans mise en demeure préalable, sanctionner un responsable de traitement dont les manquements aux obligations qui lui incombent ne sont pas susceptibles d'être régularisés, soit qu'ils*

soient insusceptibles de l'être, soit qu'il y ait déjà été remédié. » La procédure de sanction à l'encontre de l'ADEF est donc validée.
2) Concernant le caractère proportionnel de la sanction, cinq paramètres sont pris en compte par la formation restreinte pour fixer le montant de la sanction pécuniaire, à savoir :
- le caractère intentionnel ou de négligence du manquement,
- les mesures prises par le responsable du traitement pour atténuer les dommages subis par les personnes concernées,
- le degré de coopération avec la commission afin de remédier au manquement et d'atténuer ses effets négatifs éventuels,
- les catégories de données à caractère personnel concernées, et
- la manière dont le manquement a été porté à la connaissance de la commission.

Le Conseil en déduit que « *Eu égard à la nature et à la gravité du manquement constaté qu'il aurait été possible de prévenir par des mesures simples de sécurité, (…), aux moyens importants dont dispose l'association et au délai avec lequel elle a apporté les mesures correctrices de nature à remédier à ce manquement, la formation restreinte de la CNIL n'a pas infligé à l'ADEF une sanction disproportionnée en prononçant à son encontre une amende d'un montant de 75.000 euros.* »
La requête en annulation de la sanction est donc rejetée.
(Conseil d'Etat, 10è et 9è ch. réunies, ADEF c. CNIL, 17 avril 2019)

Défaut de sécurité – Le Conseil d'Etat confirme la procédure de sanction de la CNIL mais réduit son montant
Dans une décision rendue le même jour que la précédente (décision ADEF ci-dessus), le Conseil d'Etat confirme la procédure de sanction menée par la formation restreinte de la CNIL, mais considère que le montant de la sanction devait être revu à la baisse.
Une sanction pécuniaire de 250.000€ avait été prononcée à l'encontre de la société Optical Center par la CNIL le 7 mai 2018 pour manquement à son obligation de sécurité. Optical Center a par la suite décidé de contester la sanction et demander son annulation devant le Conseil d'Etat.
Le 31 juillet 2017, la CNIL a effectué un contrôle en ligne et a constaté qu'il était possible d'accéder librement, via des URL qui lui avaient été transmises, à des factures de clients d'Optical Center comprenant des données personnelles, et d'exporter un échantillon de fichiers au format .csv, sans authentification préalable. Optical Center a déclaré avoir corrigé la faille de sécurité avec son prestataire dès le 2 août 2017.
1) Concernant la procédure de sanction, les juges considèrent que, sur le fondement de l'article 45 I de la loi Informatique et Libertés modifiée (rédaction antérieure à la modification de 2018), « *la formation restreinte de la CNIL a pu légalement (…) engager, sans procéder à une mise en demeure préalable, une procédure de sanction à l'encontre de la société Optical Center.* »
2) Concernant le caractère proportionnel de la sanction, les juges rappellent dans un premier temps l'existence d'un manquement de la société Optical Center à ses obligations de sécurité prévues à la loi. Le montant de la sanction pécuniaire est proportionné à la gravité du manquement commis, sous réserve de la prise en compte des éléments mentionnés à la décision ADEF ci-dessus. En l'espèce, le Conseil estime que la CNIL n'a pas pris en compte le comportement du responsable du traitement à la suite du constat et notamment « *la célérité avec laquelle la société Optical Center a apporté les mesures correctrices de nature à remédier aux manquements constatés (…).* » Les juges, prenant en compte les circonstances de l'espèce, ont donc décidé de ramener la sanction à 200.000 euros.
(Conseil d'Etat, 10è et 9è ch. réunies, Optical Center c. CNIL, 17 avril 2019)

UNION EUROPÉENNE

Union européenne – Le Parlement européen vote pour la création d'une base de données biométrique
Le 15 avril 2019, le Parlement européen a voté en faveur de l'interconnexion de plusieurs bases de données de contrôle des frontières comprenant des données biométriques des citoyens européens et non-européens, pour créer une base unifiée de 350 millions de personnes. Cette nouvelle base de données, dénommée « Common Identity Repository » (CIR) aura pour objet de faciliter la lutte contre la criminalité et les migrations. Elle intègrera les bases existantes telles que le système d'information Schengen, Eurodac, le système d'information sur les visas (VIS) et les systèmes européens du casier judiciaire des ressortissants non-européens (ECRIS-TCN), d'entrée/sortie (EES) et d'information et d'autorisation de voyage (ETIAS).
La base CIR comprendra les données d'identité (nom, prénoms, date de naissance, numéro de passeport, etc.) et des données biométriques (empreintes digitales et numérisation faciale). Cette

base de données unifiée sera utilisée par les services de police (coopération policière et judiciaire, d'asile et de migration) et les polices aux frontières (contrôle des frontières et des visas).
La création de cette base de données unifiée est critiquée par les associations de défense de la vie privée qui craignent un suivi généralisé des déplacements des personnes, malgré l'engagement du Parlement et du Conseil européen de mettre en place des « garanties appropriées » pour protéger les droits des personnes.
On notera que la base CIR sera l'une des plus grandes bases de données de suivi des personnes au monde, derrière les systèmes mis en place par la Chine et l'Inde.
(« EU votes to create gigantic biometrics database », ZDNet, 22 avril 2019)

ROYAUME-UNI

Données des mineurs – L'ICO publie un code de bonnes pratiques pour la protection en ligne des enfants
L'autorité de contrôle britannique (Information Commissioner's Office – ICO) a publié un projet de code de bonnes pratiques pour les sites web utilisés par les mineurs de moins de 18 ans. Ce code est élaboré sur le principe de la Convention internationale des droits de l'enfant, l'objectif étant de respecter le rôle des parents et de s'adapter aux tranches d'âges des enfants et à leur capacité à faire des choix.
Le code propose une série de 16 principes à prendre en compte par les éditeurs de sites web qui collectent des données personnelles d'enfants. Parmi ces principes, on retiendra : les intérêts de l'enfant, la transparence, une utilisation des données qui ne nuise pas aux intérêts de l'enfant, un paramétrage par défaut protecteur de la vie privée, l'application du principe de minimisation des données, le non-partage des données (sauf cas exceptionnels), la désactivation par défaut de la géolocalisation.
Une analyse d'impact sur la vie privée (PIA) devrait être faite afin d'évaluer et de limiter les risques sur les données des enfants qui pourraient utiliser les services en ligne. Enfin, les fournisseurs de jouets et d'objets connectés doivent s'engager à respecter ce code.
Le RGPD s'adresse spécifiquement à la protection des données des enfants (article 8). Cette initiative de l'autorité de contrôle britannique est intéressante car elle pose une série de principes protecteurs des données des enfants, en prenant en compte leur plus grande vulnérabilité aux dérives potentielles des traitements de leurs données en l'absence d'un consentement éclairé.
(« Age appropriate design: a code of practice for online services », Site de l'ICO)

IRLANDE

Mots de passe stockés en clair - Facebook potentiellement en violation du RGPD
A la suite d'un audit interne chez Facebook, la Commission irlandaise de protection des données (IDPC) a été informée, fin avril dernier, que des centaines de millions de mots de passe d'utilisateurs de Facebook, Facebook Lite et Instagram étaient stockés en format texte sur ses serveurs. Les mots de passe étaient ainsi facilement accessibles par les employés de Facebook. L'IDPC, autorité chef de file pour la société Facebook en Europe, a annoncé avoir ouvert une enquête afin de déterminer si Facebook avait respecté ses obligations en vertu du RGPD. Plusieurs enquêtes pour manquements potentiels au RGPD sont par ailleurs menées par l'IDPC à l'encontre de la société Facebook.
(« Les millions de mots de passe Facebook exposés au cœur d'une enquête RGPD », ZDNet, 29 avril 2019)

POLOGNE

Notion d'effort disproportionné – Première sanction pécuniaire en application du RGPD
L'autorité de contrôle polonaise (UODO) a prononcé une première sanction pécuniaire le 25 mars dernier pour un montant d'environ 220.000€ à l'encontre de la société Bisnode, pour manquement à son obligation de transparence vis-à-vis de plus de 6 millions de personnes, en vertu de l'article 14 du RGPD.
La société Bisnode fournit des informations commerciales (données sur les sociétés, données de crédit, etc.) collectées principalement à partir de bases de données publiques. Ces informations comprennent des données personnelles (noms, prénoms, adresse, numéro national d'identification) de plus de 7 millions de personnes. La société a dûment informé 700.000 personnes dont elle détenait les adresses emails. Pour le reste des personnes dans la base de données, la société a estimé qu'une information par téléphone ou par courrier aurait entraîné des coûts excessifs, évalués à plus de 7,5 millions d'euros. Elle a donc décidé de publier cette information sur son site web, en application de l'article 14(5)(b) du RGPD, selon lequel l'obligation d'information est exclue si celle-ci implique des efforts disproportionnés.

Or, selon l'autorité polonaise, la société Bisnode était tenue d'informer chaque personne concernée. Elle a donc sanctionné la société pour violation de l'article 14 du RGPD.
Dans sa décision, l'autorité de contrôle omet cependant de déterminer les critères applicables à la notion d'« effort disproportionné », dans la mesure où la société Bisnode semble avoir respecté les dispositions de l'article 14(5)(b) du RGPD (« *Les paragraphes 1 à 4 ne s'appliquent pas lorsque et dans la mesure où (…) b) la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés, en particulier (…) dans la mesure où l'obligation visée au paragraphe 1 du présent article est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement. En pareils cas, le responsable du traitement prend des mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée, y compris en rendant les informations publiquement disponibles ; (…)* »
Cette décision est susceptible d'appel.
(« First fine imposed by the Polish DPA under the GDPR », Chronicle of data protection, 2 avril 2019)

INTERNATIONAL

Protection des données personnelles – La CNUCED publie une carte de l'état de la protection des données personnelles dans le monde
La CNUCED a publié une carte du monde identifiant les pays qui disposent d'une loi sur la protection des données personnelles et les pays sans protection. Le « Global Cyberlaw Tracker » permet également de visualiser les pays qui disposent de lois sur le e-commerce, sur la protection des consommateurs, sur la cybercriminalité, etc. Selon la CNUCED, à ce jour, 107 pays, dont 66 pays en voie de développement économique, ont adopté des lois de protection de données personnelles. Le taux d'adoption pour les pays d'Asie et d'Afrique est au même niveau, avec seulement 40% des pays de ces deux continents protégeant les données à caractère personnel. Des pays tels que Cuba, le Venezuela, l'Algérie, l'Egypte, le Sénégal, le Myanmar, le Laos ou le Cambodge par exemple n'ont toujours pas adopté de loi sur la protection des données personnelles.
(« Data Protection and Privacy Legislation Worldwide", UNCTAD)

AMÉRIQUE

Etats-Unis – Sanction de 5,7 millions de dollars à l'encontre de l'application TikTok pour collecte illégale de données de mineurs
TikTok est une application développée en Chine en 2016 par le groupe Bytedance. Cette application a fusionné avec son concurrent, Musical.ly courant 2018. L'application, qui permet de se filmer en dansant sur des chansons et de partager les vidéos avec ses amis, est très utilisée par les pré-adolescents et adolescents. TikTok a dépassé un milliard de téléchargements.
Le 27 février 2019, la Federal Trade Commission (FTC) a prononcé une amende de 5,7 millions de dollars à l'encontre de la société Bytedance pour collecte illégale de données personnelles de mineurs. TikTok n'aurait pas respecté l'obligation de demander l'autorisation parentale pour collecter les données personnelles des enfants, - cette obligation étant imposée par la loi COPPA pour les enfants de moins de 13 ans, d'autant plus que la société savait que son application était utilisée par un nombre très important d'enfants. TikTok a lancé une nouvelle version de l'application pour les plus jeunes, aux Etats-Unis, avec des protections spécifiques. Les données collectées illégalement devront être supprimées.
(« TikTok : amende record de 5,7 millions de dollars pour collecte illégale de données de mineurs », La Tribune, 28 février 2019)

ASIE

Vietnam – Nouvelle loi sur la cybersécurité
Une nouvelle loi sur la cybersécurité est entrée en vigueur au Vietnam le 1er janvier 2019. Cette loi, très contestée par les entreprises multinationales, a pour objet de réglementer et contrôler les contenus accessibles en ligne par les utilisateurs. La loi dispose notamment que les fournisseurs de services en ligne, qu'ils soient vietnamiens ou non, stockent les données personnelles des utilisateurs vietnamiens au Vietnam, qu'ils communiquent ces données à la demande des autorités et qu'ils modèrent les messages postés en ligne et suppriment les contenus « interdits », à savoir les contenus considérés comme critiquant le gouvernement vietnamien. La loi impose également aux opérateurs étrangers d'ouvrir des succursales ou des bureaux au Vietnam afin de faciliter la mise en œuvre des dispositions légales.
Quelques jours après son entrée en vigueur, les autorités annonçaient qu'une plateforme de réseau social avait violé la loi en matière de contrôle des contenus et des règles de publicité en ligne.

(« Asia-Pacific Data Protection and Cybersecurity Regulation », Hogan Lovells, janvier 2019, et « Vietnam criticized for 'totalitarian' law banning online criticism of governement », The Guardian, 2 janvier 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