LA LETTRE DU CABINET
TECHNOLOGIES DE L'INFORMATION

EDITO

Nous avons le plaisir de vous adresser le vingt-et-unième numéro de notre Newsletter – Technologies de l'information.

Cette lettre est organisée autour des thématiques suivantes : un flash sur la préparation pour l'entrée en application du RGPD, puis des points sur la réglementation ou la jurisprudence dans les domaines du droit de l'informatique, de l'internet, de la protection des données personnelles, de la propriété intellectuelle, des médias, de la cybersécurité, du droit fiscal.

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 ! et Bonnes fêtes !

SOMMAIRE

ⓘ FLASH – PRÉPARATIFS POUR L'ENTRÉE EN APPLICATION DU RGPD EN MAI 2018

A la une de l'actualité en ce moment figurent les préparatifs pour la mise en conformité au règlement général européen sur la protection des données (RGPD ou GDPR) qui entre en application le 25 mai 2018, soit dans à peine cinq mois.
Pour rappel, il s'agit d'une profonde réforme du droit de la protection des données personnelles qui nécessite, pour les entreprises, associations et administrations, de prendre des mesures de mise en conformité afin d'être prêt en mai 2018.
Le nouveau cadre juridique renforce les droits des personnes (consentement, droit à la portabilité des données, etc.), responsabilise davantage l'ensemble des acteurs qui traitent des données personnelles – responsables de traitement et sous-traitants, tout en leur fournissant des outils pour se mettre en conformité.
Par ailleurs, alors que la directive de 1995 et la loi Informatique et Libertés reposaient en grande partie sur les formalités préalables (déclarations, autorisations), le règlement européen repose sur une logique de conformité, avec la responsabilisation des organismes (notion d'"accountability"). Les responsables de traitements et les sous-traitants devront mettre en place des mesures de protection des données appropriées et démontrer cette conformité à tout moment.
Enfin, le montant des sanctions pour violation des dispositions du RGPD sera beaucoup plus élevé qu'actuellement, puisqu'il pourra atteindre, suivant la nature de l'infraction, entre 10 millions d'euros ou 2% du chiffre d'affaires mondial de l'entreprise, et 20 millions d'euros ou 4% du chiffre d'affaires mondial de l'entreprise…
Les membres du G29 et la CNIL ont développé plusieurs lignes directrices et outils pour clarifier les nouvelles obligations incombant aux organismes. Avocats et consultants spécialisés peuvent également conseiller les entreprises dans cette phase de mise en conformité au règlement.

INFORMATIQUE

JURISPRUDENCE

Contrat de développement – Faute du client qui n'exprime pas ses besoins
Dans un arrêt rendu le 5 octobre 2017, la cour d'appel d'Aix-en-Provence a prononcé la résiliation d'un contrat de développement de sites web aux torts du client qui n'a pas exprimé ses besoins.
En 2010, la société Nouvelles Destinations, tour-opérateur spécialisé dans la vente de séjours autour de parcs d'attractions, a souhaité refondre son site internet destiné aux professionnels (B2B) et développer un site à destination des consommateurs (B2C). Les prestations de développement ont été confiées à la société Flag Systèmes. Trois contrats ont été conclus en décembre 2010 et janvier 2011 : un contrat-cadre pour les développements spécifiques, pour un montant total de 135.000 euros, un contrat d'achat et de maintenance des licences I-Resa et un contrat d'hébergement et d'administration de la plate-forme I-Resa.

N'ayant pas reçu le dernier paiement prévu au contrat-cadre, ni le règlement des factures d'hébergement, la société Flag Systèmes a mis le client en demeure de payer le 14 octobre 2013. En réponse, la société Nouvelles Destinations a contesté devoir les sommes réclamées, invoquant divers dysfonctionnements. Le prestataire a donc fait assigner la société Nouvelles Destinations et son assureur devant le tribunal de commerce d'Aix-en-Provence en règlement des sommes. Dans un jugement du 10 novembre 2015, le tribunal a condamné la société Nouvelles Destinations à régler les sommes dues à la société Flag Systèmes. Nouvelles Destinations a interjeté appel.
Dans sa décision du 5 octobre 2017, la Cour relève que le contrat-cadre rappelle en préambule que la société Nouvelles Destinations n'a pas fourni de document d'expression de ses besoins ni de cahier des charges, que le contrat-cadre est destiné à permettre "d'initialiser les premières phases de travail sans que les enveloppes définitives soient engagées", et qu'il est recommandé à la société Nouvelles Destinations « *de recourir à une assistance à maîtrise d'ouvrage, mener une réflexion de fond sur l'organisation des services, les processus métiers et les flux d'informations mis en place, et la mise en place d'un comité de pilotage*. » Or, la société Nouvelles Destinations n'a suivi aucune des recommandations du prestataire.
Par ailleurs, alors qu'il revient à la société cliente de prouver les dysfonctionnements allégués et leur imputabilité au prestataire, les juges relèvent que la société Nouvelles Destinations ne produit que des emails émanant d'elle-même, se plaignant de dysfonctionnements, sans aucune plainte de clients ou de partenaires commerciaux, ni constat objectif desdits dysfonctionnements pouvant justifier le non-paiement des factures du prestataire.
En conséquence, la Cour a confirmé le jugement du tribunal de commerce, mais revu la condamnation à la baisse. La société Nouvelles Destinations a ainsi été condamnée à payer 101.000 euros dus au titre des contrats.
(CA d'Aix-en-Provence, 8e ch. B, arrêt du 5 octobre 2017 Nouvelles Destinations / Flag Systèmes et Hiscox Europe Underwriting Ltd)

Contrat de développement – Résiliation du contrat aux torts du client ayant refusé la recette provisoire
Dans un arrêt du 6 juillet 2017, la cour d'appel de Grenoble a confirmé la résiliation d'un contrat de développement d'un site internet aux torts exclusifs du client qui avait refusé de procéder à la réception provisoire, alors que la réception aurait pu lui permettre de faire réaliser au prestataire les corrections nécessaires au vu des éventuelles réserves.
La société Sikirdji Gemfrance, spécialisée dans le commerce de pierres fines et précieuses a conclu un contrat de réalisation de site web avec la société DediServices le 9 juillet 2012 et a versé un premier acompte de 40% à la commande (soit 10.697,02€ TTC). Prétendant que le site commandé n'avait jamais été achevé et qu'il comportait de nombreux dysfonctionnements, la société Sikirdji Gemfrance a demandé au prestataire le remboursement de l'acompte versé par mise en demeure du 4 avril 2013, puis assigné la société DediServices en résolution du contrat et remboursement de l'acompte le 16 septembre 2013. Dans son jugement du 28 novembre 2014, le tribunal de commerce de Grenoble a condamné la société cliente à payer à la société DediServices la somme de 16.045,54 € au titre des factures impayées avec application des pénalités de retard contractuelles, 10.000 € euros de dommages et intérêts et 2.000 € au titre de l'article 700 du code de procédure civile. La société Sikirdji Gemfrance a interjeté appel le du 16 janvier 2015.
Les juges d'appel relèvent que le site développé par la société DediServices n'a pas fait l'objet d'une réception provisoire, comme prévu au contrat, la société Sikirdji Gemfrance ayant refusé la réception provisoire du site, alors que la réception avait notamment pour objet d'obliger le prestataire à faire les modifications correspondant aux éventuelles réserves mentionnées au procès-verbal de recette.
La cour a confirmé la condamnation de la société Sikirdji Gemfrance à payer au prestataire les sommes prévues par le contrat et non encore réglées, augmentées des pénalités de retard, 10.000 € pour le travail supplémentaire généré par les nombreuses demandes d'interventions et de modifications, et 50.000 € de dommages-intérêts.
Cet arrêt fait l'objet d'un pourvoi en cassation et n'est donc pas définitif.
(CA Grenoble, ch. com, arrêt du 6 juillet 2017 Sikirdji Gemfrance / DediServices)

Développement informatique – L'employeur doit prouver l'effacement des codes sources par son ex-salarié par une expertise contradictoire
L'employeur qui allègue qu'un ex-salarié est parti en rendant les codes sources des logiciels de l'entreprise inexploitables doit le prouver par une expertise contradictoire.
La société Kappa Engineering est éditeur de logiciels d'assistance à l'exploitation pétrolière. A la suite du licenciement de l'ingénieur en charge des développements sur une gamme de ses logiciels, devant

être commercialisée courant 2016, son successeur sur le projet a constaté qu'une partie du code source manquait et que le code laissé par son prédécesseur avait été rendu illisible par obfuscation, empêchant toute possibilité de modification et de maintenance du logiciel.
La société Kappa Engineering a obtenu, sur requête le 1er février 2016, la désignation d'un huissier afin de procéder à des constatations dans ses propres locaux.
La société Kappa Engineering a par la suite été autorisée à assigner son ancien salarié d'heure à heure devant le juge des référés du tribunal de grande instance de Grasse le 1er mars 2016, au motif que celui-ci n'avait pas enregistré dans la base de données de la société les codes source indispensables à l'évolution et à la maintenance du logiciel sur lequel il travaillait et avait rendu du code illisible.
Le 4 avril 2016, le tribunal de grande instance de Grasse a condamné l'ex-salarié à restituer à la société Kappa Engineering les codes source dépourvus de toute obfuscation ou de toute autre technique visant à complexifier leur lecture ou à effectuer toute procédure utile afin de rendre lisible le code source des logiciels dans leur dernière version au moment de son licenciement.
Par un arrêt du 30 mars 2017, la cour d'appel d'Aix-en-Provence a constaté la nullité de l'expertise et prononcé la rétractation de l'ordonnance sur requête. Dans un second arrêt du 16 novembre 2017, la cour d'appel a infirmé l'ordonnance de référé ayant condamné l'ex-salarié à restituer les codes sources, rejetant le rapport d'expertise privée au motif qu'il n'avait pas été établi de manière contradictoire, en présence de l'ex-salarié : *« les développements contradictoires des parties sur des faits faisant appel à des technologies complexes ne permettent pas au juge des référés, juge de l'évidence, de caractériser l'existence d'un trouble manifestement illicite, de sorte que M. X. ne peut être contraint à procéder à des opérations de "remise en état" des logiciels en cause »*.
Jugeant par ailleurs que *« l'urgence n'est pas un critère suffisant pour contrevenir au principe fondamental de la contradiction »*, la cour a estimé que les nouvelles pièces (constat d'huissier et rapport d'un consultant) produites par la société Kappa Engineering n'étaient pas de nature à établir un dommage imminent, d'autant que le salarié nie les faits reprochés, ni un trouble manifestement illicite justifiant la mesure d'intervention de ce dernier, dans la mesure où sa responsabilité n'est nullement démontrée. Selon la cour, les accusations à l'encontre de l'ex-salarié de la société Kappa Engineering reposent sur un constat d'huissier réalisé sur les analyses effectuées le même jour par un expert privé. Or, ce rapport ne peut avoir la valeur de celui d'une expertise contradictoire. En conséquence, l'ordonnance de référé a été infirmée.
(CA d'Aix-en-Provence, 1ère ch. C, arrêt du 30 mars 2017 M. X. / SA Kappa Engineering)

INTERNET

RÉGLEMENTATION

Plateformes internet – Publication de trois décrets pour "favoriser la transparence des plateformes numériques"
Trois décrets, pris en application de la loi pour une République numérique, « pour favoriser la transparence des plateformes numériques » ont été publiés le 29 septembre 2017. Ces décrets concernent les moteurs de recherche, les réseaux sociaux et les sites comparateurs ainsi que les places de marchés et les sites d'économie collaborative.
A compter du 1er janvier 2018, les plateformes qui valorisent des contenus, des biens ou des services proposés par des tiers (moteurs de recherche, sites comparatifs) préciseront "*les critères de référencement et de classement"* et devront ainsi indiquer dans quelle mesure le montant de leur rémunération entre en compte dans l'ordre de présentation des contenus. De même, les sites publiant des avis de consommateurs devront préciser s'ils ont été vérifiés et, le cas échéant, de quelle manière cette vérification a été effectuée.
Par ailleurs, les places de marchés et sites d'économie collaborative devront fournir des informations essentielles qui peuvent orienter les choix des consommateurs et qui ne sont pas toujours précisées ou accessibles, telles que la qualité du vendeur (professionnel ou particulier), le montant des frais de mise en relation facturés par la plateforme (commission), l'existence ou non d'un droit de rétractation, l'existence ou non d'une garantie légale de conformité ou encore les modalités de règlement des litiges.
Enfin, à compter du 1er janvier 2019, les plateformes qui comptabilisent plus de 5 millions de visiteurs uniques mensuels devront "*appliquer des bonnes pratiques en matière de clarté, de transparence et de loyauté. »* Ces règles devront être consultables en ligne.
(Décret n°2017-1434 du 29 septembre 2017 relatif aux obligations d'information des opérateurs de plateformes numériques ; Décret n°2017-1435 du 29 septembre 2017 relatif à la fixation d'un seuil de

connexions à partir duquel les opérateurs de plateformes en ligne élaborent et diffusent des bonnes pratiques pour renforcer la loyauté, la clarté et la transparence des informations transmises aux consommateurs ; Décret n°2017-1436 du 29 septembre 2017 relatif aux obligations d'information relatives aux avis en ligne de consommateurs)

Plateformes internet – La Commission européenne publie de nouvelles lignes directrices pour la suppression des discours haineux et du contenu lié au terrorisme

Le 28 septembre 2017, la Commission européenne a publié de nouvelles lignes directrices pour les plateformes en ligne, visant à renforcer la prévention, la détection et la suppression des contenus répréhensibles, et plus particulièrement les discours haineux et le contenu lié au terrorisme.

Rappelant que l'apologie du terrorisme et les discours haineux sont illicites en droit communautaire, le communiqué de la Commission indique attendre des plateformes en ligne qu'elles prennent des mesures rapides au cours des prochains mois, sachant que si les entreprises de technologie ne mettent pas en œuvre ces lignes directrices, la Commission "*évaluera si des mesures supplémentaires sont nécessaires ... y compris de possibles mesures législatives afin de compléter le cadre réglementaire existant*", et ce, même si la réglementation actuelle leur impose déjà de supprimer les contenus manifestement illicites. Ses travaux s'achèveront en mai 2018.

Les lignes directrices couvrent trois étapes : la détection des contenus litigieux et la notification, leur suppression efficace et la prévention de leur réapparition. Pour la détection, la Commission attend des plateformes i) qu'elles coopèrent plus étroitement avec les autorités nationales compétentes en désignant des points de contact, ii) qu'elles mettent en place des systèmes automatisés de détection, et iii) qu'elles travaillent avec des acteurs fournissant des signalements "de confiance" et disposant d'une expertise sur les contenus illégaux.

Pour une "suppression efficace", les entreprises peuvent être assujetties à des délais (non encore précisés) lorsqu'un "préjudice grave est en jeu".

Enfin, les entreprises devraient introduire des mesures de protection pour prévenir un "retrait excessif", et développer des outils plus automatisés pour éviter que le contenu illégal ne réapparaisse après sa suppression.

(Microsoft, Facebook, Twitter and Google submit to EU hate speech rules, in ZD Net, 31 mai 2016 ; et Commission européenne - Communiqué de presse, « Union de la sécurité : La Commission redouble d'efforts pour lutter contre le contenu illicite en ligne », Bruxelles, le 28 septembre 2017)

Blockchain – Le Ministère de l'économie et des finances propose un projet d'ordonnance

Après une consultation lancée entre mars et mi-mai 2017 sur la transmission de certains titres financiers via la blockchain, dont la synthèse a été publiée courant septembre, le Ministère de l'économie et des finances a proposé un projet d'ordonnance. Ce texte viendrait à la suite de la loi Sapin II du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, dont les dispositions permettent notamment d'adapter le droit applicable à certains titres financiers au moyen d'un dispositif d'enregistrement électronique partagé, ou « technologie de registre distribué » (distributed ledger technology ou DLT).

Bien qu'il soit déjà possible d'utiliser une technologie de registre distribué pour la transmission de titres, de nombreuses zones d'insécurité juridique persistent, y compris concernant le droit applicable en matière de propriété du titre et les modalités de règlement.

La majorité des parties prenantes ayant répondu à la consultation estime souhaitable de prévoir un cadre juridique où « *l'intervention du législateur se limiterait à assurer la neutralité technologique des exigences de fond pesant sur les acteurs existants* ». Ainsi, la blockchain a besoin d'un cadre juridique, mais a minima. Le projet de texte, intitulé « Ordonnance relative à la transmission et la représentation de titres financiers au moyen d'un dispositif d'enregistrement électronique partagé » aura pour objet de reformer le Code monétaire et financier pour fournir un cadre juridique aux opérations réalisées par l'intermédiaire de cette technologie.

(Ministère de l'économie et des finances, Direction générale du Trésor,Consultation publique: Projet d'ordonnance blockchain/titres financiers)

JURISPRUDENCE

Internet – Une société condamnée pour l'insertion de backlinks détournant une partie du trafic internet de son concurrent vers son propre site

Les sociétés IES et Autoconfiance 25 sont mandataires automobiles. La première a été condamnée le 17 octobre 2017 par le tribunal de commerce de Belfort pour la mise en place d'un système de redirection de liens destinés à détourner une partie du trafic du site web de son concurrent vers son

propre site, et ce même si ce système de backlinks a été mis en place par son prestataire, à l'insu de la société IES.
Mi-novembre 2015, la société Autoconfiance 25 a constaté une baisse de trafic sur son site internet et de ses contacts clients. Après des recherches, Autoconfiance 25 a découvert que la baisse de trafic était due à un détournement de clientèle vers le site internet de la société IES, les mots clés « autoconfiance » et dérivés saisis sur le moteur de recherche Google aboutissant à des résultats renvoyant vers le site internet d'IES.
Par courrier recommandé du 25 novembre 2015, Autoconfiance 25 a mis en demeure la société IES de cesser toute utilisation des signes « autoconfiance » et dérivés et a proposé un règlement amiable par le versement d'une somme forfaitaire de 20.000 euros pour couvrir le préjudice estimé. La société IES a répondu avoir demandé à son prestataire de référencement, la société Effiliation l'arrêt des redirections des liens litigieux vers son propre site internet, le jour même de la découverte. IES ajoute que le préjudice subi se limiterait à 1 358 clics et un « lead ».
Le tribunal constate que la société Effiliation prestataire en référencement internet de la société IES, a fait mettre en place un système de redirection de liens (backlinks) non conformes aux bonnes pratiques, détournant ainsi un partie du trafic vers le site internet de la société IES. Il en conclut que de telles pratiques sont constitutives d'une faute et faussent ainsi le jeu normal du marché. Le tribunal retient ainsi la responsabilité de la société IES pour la mise en place d'une politique de référencement trompeuse, par l'intermédiaire de son prestataire Effiliation, ces faits étant constitutifs d'un acte de concurrence déloyale et parasitaire.
La société IES a été condamnée à verser 38.941€ à son concurrent en réparation du préjudice résultant de la perte de chance d'être plus amplement visité.
(Tribunal de commerce de Belfort, jugement du 17 octobre 2017, Autoconfiance 25 / Société IES)

Moteurs de recherche - Le Conseil d'Etat interroge la CJUE sur la portée territoriale du droit au déréférencement
Le 13 mai 2014, la Cour de justice de l'Union européenne (CJUE) a consacré le « droit au déréférencement ». Ce droit permet à toute personne résidant sur le territoire de l'UE de demander aux moteurs de recherche le déréférencement de liens renvoyant vers des contenus comprenant des données personnelles les concernant.
Cette décision de la CJUE pose cependant des difficultés sérieuses d'interprétation quant à la détermination du champ d'application territorial des obligations de déréférencement pesant sur l'exploitant d'un moteur de recherche. En effet, le déréférencement porte-t-il uniquement sur l'extension du pays de résidence du demandeur (par exemple google.fr, google.it, ou google.de), ou sur les extensions des Etats-membres, à l'exclusions du reste du monde, ce qui limite alors de manière substantielle la portée de ce droit ?
Le 10 mars 2016, la formation restreinte de la CNIL a prononcé une sanction de 100.000 euros à l'encontre de la société Google Inc. suite au refus de la société de respecter la mise en demeure de la CNIL de procéder au déréférencement sur l'intégralité des extensions du nom de domaine de son moteur de recherche. La société Google Inc. a formé un recours devant le Conseil d'Etat en annulation de la délibération de la CNIL.
Le 19 juillet 2017, le Conseil d'Etat a sursis à statuer sur la requête de Google et interrogé la CJUE afin de préciser la portée territoriale de l'obligation de déréférencement par les moteurs de recherche.
(Conseil d'Etat, (9e et 10e sous-sections réunies), 19 juillet 2017, Sté Google Inc. ; Arrêt de la Cour (grande chambre) du 13 mai 2014, Google Spain SL et Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González ; Délibération de la formation restreinte n° 2016-054 du 10 mars 2016 prononçant une sanction pécuniaire à l'encontre de la société Google Inc.)

PROTECTION DES DONNÉES PERSONNELLES

RÉGLEMENTATION

RGPD – Projet de loi relatif à la protection des données personnelles : la CNIL publie son avis
Le 30 novembre 2017, la CNIL a rendu son avis sur le projet de loi relatif à la protection des données personnelles. Ce texte modifie la loi Informatique et Libertés afin de permettre la mise en œuvre effective du « paquet européen de protection des données » adopté le 27 avril 2016, comprenant le Règlement général sur la protection des données (RGPD) et de la Directive sur la prévention et la détection des infractions pénales (Directive UE 2016/680).
Le projet de loi est composé de cinq titres, dont le premier concernant les dispositions communes au RGPD et à la Directive sur la prévention et la détection des infractions pénales, le second concernant

les dispositions du RGPD permettant des marges de manœuvre aux Etats membres pour prendre des mesures spécifiques, et le troisième concernant les dispositions relatives à la transposition de la Directive sur la prévention et la détection des infractions pénales.
Trois points à retenir :

- ce texte va dans le sens de l'harmonisation recherchée par le RGPD et ne maintient des dérogations nationales que lorsque celles-ci sont réellement justifiées, particulièrement en matière de données de santé (modification du chapitre IX de la loi Informatique et Libertés) ;
- l'étendue des pouvoirs de contrôle de la CNIL et les modalités de réalisation d'opérations conjointes avec d'autres autorités européennes sont précisées ;
- la CNIL relève que d'autres propositions n'ont pas été retenues dans ce projet, concernant notamment le renforcement des garanties lors de l'utilisation de traitements algorithmiques débouchant sur l'adoption de décisions administratives, ou l'adaptation de ses procédures pour permettre à la Commission de faire face à l'augmentation d'activité liée à la nouvelle réglementation.

Enfin, ce projet de loi ne prend en compte que des dispositions « a minima », nécessaires à la mise en œuvre du Règlement et de la Directive. Il est prévu que l'ensemble de la loi Informatique et Libertés du 6 janvier 1978 soit refondue par voie d'ordonnance à venir, avant la date du 25 mai 2018 (art. 20 du projet de loi).
(Projet de loi relatif à la protection des données personnelles (JUSC1732261L) ; et CNIL, Délibération n°2017-299 du 30 novembre 2017 portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n°78-17 du janvier 1978)

PRÉPARATION À LA MISE EN CONFORMITÉ AU RGPD (GDPR)

La CNIL publie des recommandations sur la procédure de notification d'incidents de sécurité aux autorités

Avec l'entrée en application du RGPD, tous les organismes seront désormais soumis à une obligation de notification des violations de données personnelles à la CNIL (art. 33 et 34 RGPD). Le 26 juillet 2017, la CNIL a publié des recommandations relatives à la procédure de notification d'incidents de sécurité aux autorités.
En cas d'une violation de données, l'organisme doit porter à la connaissance de la CNIL, via un nouveau téléservice, qui sera opérationnel en mai 2018, les éléments suivants :

- la description de la nature de la violation de données à caractère personnel ;
- les catégories de données concernées ;
- le nombre approximatif de personnes concernées par la violation ;
- les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations peuvent être obtenues, la description des conséquences probables de la violation de données et les mesures prises ou à prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Par ailleurs, en cas de risque élevé pour les personnes concernées, le responsable de traitement doit également informer les utilisateurs touchés par l'incident, sauf si le responsable a pris, préalablement ou postérieurement à la violation, des mesures techniques ou organisationnelles appropriées.
(Site de la CNIL)

Analyse d'impact relative à la protection des données : lignes directrices publiées par le G29 et logiciel mis à disposition par la CNIL

L'article 35 du RGPD prévoit la conduite d'une analyse d'impact sur la protection des données (ou DPIA) lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées. Cette analyse d'impact doit faire apparaître les caractéristiques du traitement, les risques et les mesures adoptées.
Afin d'expliquer l'article 35 et en proposer une interprétation commune, le groupe du G29 (« CNIL européennes ») a adopté des "*lignes directrices sur les DPIA et les traitements susceptibles d'engendrer des risques élevés*", dont la version définitive a été publiée le 4 octobre 2017. Ce document inclut une infographie, expliquant les principes des DPIA et une foire aux questions (FAQs) afin de fournir des réponses pratiques et en français sur le sujet.

Par ailleurs, la CNIL prépare des outils pour aider les professionnels à définir dans quels cas une analyse d'impact est obligatoire et les accompagner dans sa réalisation. A ce titre, la Commission vient de mettre à disposition un logiciel libre pour accompagner les organismes dans l'analyse

d'impact sur la protection des données.
Ce logiciel (disponible en français et en anglais) déroule l'intégralité de la méthode PIA développée par la CNIL. L'application de cette méthode permet d'être conforme aux exigences définies dans les lignes directrices du G29. Actuellement présenté en version bêta, des améliorations et enrichissements pourront être apportés au logiciel en fonction des retours utilisateurs qui pourront également développer de nouvelles fonctionnalités et les partager par la suite avec la communauté.
(Guidelines on Data Protection Assessment (DPIA) and determining whether data processing is "likely to result in a high risk" for the purposes of regulation 2016:679, last revised and adopted on 4 October 2017, 17/EN WP248 rev 0.1 ; RGPD : un logiciel pour réaliser son analyse d'impact sur la protection des données (PIA), CNIL, 22 novembre 2017)

Le G29 publie des lignes directrices sur la décision individuelle automatisée et le profilage
Le groupe du G29 a publié le 3 octobre 2017, de nouvelles lignes directrices sur la décision individuelle automatisée et le profilage (art. 22 RGPD).
Les membres du G29 reconnaissent que la pratique des décisions individuelles automatisées et du profilage peut être utile tant pour les personnes concernées que pour les organismes, grâce à une plus grande efficacité et une économie de ressources, mais ils craignent que ces pratiques créent des risques importants pour les personnes.
Le texte distingue entre la procédure de décision individuelle automatisée et la procédure de profilage. La procédure de décision individuelle automatisée concerne la possibilité de prendre des décisions par le biais de moyens technologiques en l'absence d'intervention humaine. La procédure de profilage concerne la collecte de données personnelles et l'analyse de leurs caractéristiques ou des modèles de comportement aux fins de les classer et/ou de faire des prédictions ou évaluations sur i) leur capacité à réaliser certaines tâches, 2) leurs intérêts, ou 3) leur comportement probable.
Même si ces deux procédures sont distinctes, une décision individuelle automatisée peut facilement déboucher sur du profilage.
Les lignes directrices donnent des orientations sur le droit de ne pas être soumis à une décision basée uniquement sur une procédure de décision individuelle automatisée, le droit d'information et d'accès, et les audits.
(Guidelines on automated individual decision making and profiling for the purposes of regulation 2016/679 adopted on 3 October 2017, 17/EN WP251)

La CNIL publie un guide pour accompagner les sous-traitants
Les sous-traitants qui traitent des données personnelles pour le compte de leurs clients ont de nouvelles responsabilités au regard du Règlement européen sur la protection des données (RGPD). La CNIL publie un guide pour les sensibiliser et les accompagner dans la mise en œuvre de leurs obligations.
Les sous-traitants seront tenus de respecter des obligations spécifiques en matière de sécurité, de confidentialité et de documentation de leur activité. Ils devront prendre en compte la protection des données dès la conception du service ou du produit et par défaut, tenir un registre des activités de traitement effectuées pour le compte de leurs clients et le cas échéant, désigner un délégué à la protection des données (DPD) dans les mêmes conditions qu'un responsable de traitement.
Les sous-traitants ont notamment une obligation de conseil auprès de leurs clients, responsables de traitement. Ils doivent les aider dans la mise en œuvre de certaines obligations du règlement (étude d'impact sur la vie privée, notification de violation de données, sécurité, contribution aux audits).
Les sous-traitants concernés sont notamment : les prestataires de services informatiques (hébergement, maintenance, …), les intégrateurs de logiciels, les sociétés de sécurité informatique, les entreprises de service du numérique (ESN, ex-SSII) qui ont accès aux données, les agences de marketing ou de communication qui traitent des données personnelles pour le compte de leurs clients.
(Règlement européen sur la protection des données : un guide pour accompagner les sous-traitants, 29 septembre 2017, site de la CNIL)

La CNIL donne des conseils sur la tenue du registre des traitements
Avec le RGPD, la grande majorité des traitements mis en oeuvre n'auront plus besoin d'être déclarés à l'autorité de contrôle. En revanche, le responsable de traitement sera soumis à une obligation globale d"accountability" (responsabilité). Il devra notamment pouvoir, à tout moment, démontrer sa conformité au règlement.
Le registre des traitements est l'un des documents qui permettra de démontrer la conformité d'une entreprise en cas de contrôle de la CNIL (art 30 RGPD). Le registre est tenu par le Délégué à la protection des données (DPD ou DPO). Il mentionne le nom et les coordonnées du responsable du

traitement, les finalités du traitement (relations commerciales, gestion RH, etc.), les catégories de personnes concernées (clients, salariés, candidats), les acteurs, internes ou externes, amenés à gérer ces données, le parcours des flux de données en cas de transferts hors de l'Union européenne, les délais de conservation des données et la description des mesures de sécurité techniques et organisationnelles prises pour en assurer leur protection.
Les informations à inscrire au registre comprennent, en outre, les notions de protection des données dès la conception ("privacy by design") et de protection par défaut ("privacy by default"). Il devient donc nécessaire, avant la mise en oeuvre de nouveaux traitements, de s'interroger sur la nécessité du traitement, le type de données nécessaires au traitement, le caractère légitime de la finalité, le lieu de stockage des données, la durée de conservation des données, et le cas échéant, la nécessité de réaliser une analyse d'impact (DPIA), d'identifier les sous-traitants et les lieux de traitement (UE ou hors UE).
Un modèle de registre est proposé par la CNIL sur son site.
(Site de la CNIL)

La CNIL met à jour ses labels Formation et Gouvernance
Il y a quelques années, la CNIL avait développé une activité de labellisation autour de quatre référentiels :
- Le label "Formation", qui garantit un haut niveau de qualité en matière de formations informatique et libertés,
- Le label "Coffre-fort numérique", qui atteste d'un service respectueux de l'intégrité, de la disponibilité et de la confidentialité des données stockées par les particuliers ou les professionnels,
- Le label "Procédures d'audit informatique et libertés", qui s'applique à la procédure utilisée pour vérifier que ces traitements sont conformes à la loi Informatique et Libertés,
- Le label "Gouvernance", qui s'applique à l'ensemble des mesures, règles et bonnes pratiques permettant la gestion des données à caractère personnel d'un organisme.

Ces labels ont été développés en tenant compte de la loi Informatique et Libertés. Il était donc nécessaire de les mettre à jour afin d'intégrer les exigences du RGPD. La CNIL vient ainsi d'actualiser les labels "Formation" et "Gouvernance Informatique et Libertés". La mise à jour des labels "Procédure d'audit" et "Coffre-fort numérique" doit intervenir prochainement.
(Site de la CNIL)

JURISPRUDENCE, AVIS ET RECOMMANDATIONS

Jouets connectés – La CNIL met en demeure la société Genesis Industries Ltd pour défaut de sécurité
Le 20 novembre 2017, la Présidente de la CNIL a mis en demeure la société Genesis Industries Ltd, sise à Hongkong, de procéder à la sécurisation de jouets connectés (poupée « My Friend Cayla » et robot « I-QUE »).
Les jouets sont équipés d'un microphone et d'un haut-parleur et sont associés à une application téléchargeable. Ces jouets répondent aux questions posées par les enfants sur divers sujets. La réponse est extraite d'internet par l'application.
Alertée, en décembre 2016, par une association de consommateurs sur le défaut de sécurité des deux jouets, la CNIL a réalisé des contrôles en ligne en janvier et novembre 2017. Ces contrôles ont permis de relever que la société collecte une multitude d'informations personnelles sur les enfants et leur entourage : les voix, le contenu des conversations échangées avec les jouets, mais également des informations renseignées dans un formulaire de l'application « My Friend Cayla App ».
Plusieurs manquements à loi Informatique et Libertés ont été constatés dont notamment le non-respect de la vie privée des personnes en raison d'un défaut de sécurité (une personne située à 9 mètres des jouets à l'extérieur d'un bâtiment, peut connecter un téléphone mobile aux jouets via Bluetooth sans avoir à s'authentifier) et le défaut d'information des utilisateurs des jouets. La Présidente de la CNIL a donc décidé de mettre en demeure la société Genesis Industries Ltd de se conformer à la loi Informatique et Libertés dans un délai de deux mois.
Cette mise en demeure n'est pas une sanction : aucune suite ne sera donnée à cette procédure si la société se conforme à la loi dans le délai imparti. Dans ce cas, la clôture de la procédure fera l'objet d'une publicité. En revanche, si la société ne se conforme pas à cette mise en demeure dans le délai imparti, la Présidente pourra désigner un rapporteur qui proposera le cas échéant à la formation restreinte de la CNIL de prononcer une sanction.
(CNIL, Décision n°MED-2017-073 du 20 novembre 2017 mettant en demeure la société Genesis Industries Limited)

PROPRIÉTÉ INTELLECTUELLE

JURISPRUDENCE

Contrefaçon – Un particulier lourdement condamné pour vente de contrefaçons de logiciels sur eBay

Dans un jugement correctionnel du TGI de Limoge du 11 juillet 2017, un particulier qui avait vendu 289 exemplaires de logiciels Adobe sur eBay entre décembre 2013 et mars 2016 a été condamné à six mois de prison avec sursis, deux ans de mise à l'épreuve et à verser 664.411 euros de dommages et intérêts à l'éditeur, la société Adobe Systems Inc.

Le prévenu était poursuivi pour avoir reproduit sans autorisation la suite de logiciels CSS d'Adobe (comprenant Photoshop, Dreamweaver, Indesign, Creative Suite, Flash Professional et Illustrator) en 289 exemplaires, pour avoir reproduit la marque Adobe pour les besoins de leur distribution illicite sur la plateforme eBay, et pour avoir exercé une activité à but lucratif sans être immatriculé au répertoire des métiers ou des entreprises ou au registre du commerce et des sociétés. Les revenus de la vente s'élèvent à 31.867 euros.

Le prévenu a été déclaré responsable du préjudice subi par la société Adobe Systems Inc. Adobe demandait près d'un million d'euros en réparation du préjudice causé par la contrefaçon de marques et de droits d'auteurs. Le tribunal lui a accordé la somme de 664.411 euros, cette somme correspondant à 289 ventes de logiciel pour un coût unitaire de 2.299 euros.

(TGI de Limoges, jugement correctionnel du 11 juillet 2017 Adobe Systems Inc. / M. X.)

MÉDIAS

RÉGLEMENTATION

Marché unique – Nouveau règlement relatif à la portabilité transfrontalière des services de contenu en ligne

Le 8 juin 2017, le Conseil de l'Union européenne et le Parlement ont adopté un nouveau règlement relatif à la portabilité transfrontalière des services de contenu en ligne dans le marché intérieur.

Ce règlement garantit aux citoyens de l'Union européenne, qui ont légalement souscrit des abonnements en ligne pour des services de contenu (tels Netflix et Spotify) dans leur Etat membre de résidence, de pouvoir continuer à accéder et à utiliser ces services lorsqu'ils voyagent et sont présents temporairement dans un autre Etat membre.

L'objet de ce règlement est de permettre de remédier aux problèmes des licences territoriales et d'exclusivité applicables à la fourniture de services de contenu en ligne au sein de l'Union européenne et d'éviter les situations de blocage géographique. Les fournisseurs de services de contenu en ligne devront ainsi permettre à leurs abonnés qui résident dans un Etat membre d'utiliser leur abonnement et d'accéder au contenu licite qu'ils ont acquis ou loué, sur la même gamme d'appareils et avec le même éventail de fonctionnalités, lorsqu'ils voyagent dans l'Union européenne et sont présents temporairement dans un autre Etat membre. L'obligation de portabilité ne fera pas l'objet d'une licence distincte ou d'une renégociation des licences existantes entre les titulaires de droits et les fournisseurs de services.

Le règlement s'applique uniquement aux services de contenu payants, tels que les services audiovisuels, la musique et les livres électroniques, les événements sportifs et autres émissions télévisées, que les opérateurs commerciaux proposent en ligne par streaming, téléchargement ou tout autre moyen technique licite, sur la base de la portabilité, sans se limiter à un emplacement spécifique, et par abonnement. Les services en ligne gratuits proposés par les opérateurs qui choisissent de mettre en place des services de portabilité et acceptent de vérifier l'Etat membre de résidence de leurs abonnés peuvent également permettre la portabilité de leurs services. Le règlement interdit aux fournisseurs de services de réduire la qualité de la prestation du service.

Le règlement entre en application le 20 mars 2018.

(Règlement (UE) 2017/1128 du Parlement européen et du Conseil du 14 juin 2017, relatif à la portabilité transfrontière des services de contenu en ligne dans le marché intérieur)

CYBERSÉCURITÉ

Cybermalveillance - Un guichet unique pour les particuliers, PME et collectivités territoriales

Après une phase d'expérimentation, la plateforme Cybermalveillance.gouv.fr, dispositif vers lequel peuvent désormais se tourner les victimes de cybermalveillance, a été lancé sur l'ensemble du

territoire national le 17 octobre 2017. Il s'agit d'un guichet unique qui met en relation les victimes (particuliers, entreprises (PME/TPE) et collectivités territoriales - hors OIV) avec des prestataires de proximité, compétents et présents sur l'ensemble du territoire national, des administrations de l'État (Gendarmerie, Police, représentants locaux de l'ANSSI) ou des collectivités et acteurs locaux (chambres consulaires, fédérations professionnelles, réseaux « transition numérique », etc.).
Les objectifs de cette plateforme sont :
- la mise en relation des victimes via la plateforme numérique avec des prestataires de proximité susceptibles de restaurer leurs systèmes ;
- la mise en place de campagnes de prévention et de sensibilisation à la sécurité du numérique ;
- la création d'un observatoire du risque numérique permettant de l'anticiper.
La plateforme propose également plusieurs outils et démarches de sensibilisation aux cyber-risques : principes de base à respecter pour assurer sa cyber sécurité, guides de bonnes pratiques en matière de cyber sécurité.
Ce dispositif est incubé par l'ANSSI et copiloté avec le ministère de l'Intérieur.
(plateforme Cybermalveillance.gouv.fr)

FISCAL

RÉGLEMENTATION

TVA – Obligation d'utiliser un logiciel de comptabilité certifié
A compter du 1er janvier 2018, les organismes assujettis à la TVA devront obligatoirement utiliser un logiciel de comptabilité ou de gestion enregistrant les règlements clients, conforme aux exigences de l'article 286 3° bis du Code général des impôts, à savoir un logiciel ou un système satisfaisant à des conditions d'inaltérabilité, de sécurisation, de conservation et d'archivage des données, permettant à l'administration fiscale d'effectuer des contrôles. L'absence d'archivage pourrait conduire à la remise en cause de la sincérité de la comptabilité.
Le système utilisé devra être certifié soit par un organisme accrédité, soit par une attestation individuelle de l'éditeur du logiciel conforme à un modèle donné par l'administration.
Sont directement concernés les éditeurs de logiciels, les fabricants des systèmes de caisse mais aussi les entreprises et les auto-entrepreneurs assujettis. Cette nouvelle obligation, qui prévoit de lourdes sanctions en cas de manquement, s'inscrit dans le plan gouvernemental de lutte antifraude à la TVA.
(art. 286 3° bis du CGI)

E-commerce – Nouvelle taxe sur les entrepôts e-commerce et les « drives » proposée par le Sénat
À l'occasion de l'examen du projet de loi de finances pour 2018, le Sénat vient d'adopter, contre l'avis du gouvernement, un amendement visant à créer une nouvelle taxe sur les entrepôts des sociétés de e-commerce et les « drives » de plus de 400 m2.
Cette taxe, proportionnelle au chiffre d'affaires par mètre carré, et à la surface de stockage, pourrait atteindre 34,12 euros par m2 pour « les locaux destinés au stockage des biens vendus par voie électronique » ou de drive.
Cette taxe frapperait tous les commerces utilisant internet. Elle entraînerait en outre non seulement une distorsion de concurrence entre les sociétés de e-commerce, au détriment de celles qui utilisent des entrepôts de stockage en France - tout e-commerçant vendant en France, à partir d'entrepôts situés à l'étranger serait exempté de la taxe, mais également un risque socio-économique – délocalisation des plateformes logistiques et licenciements associés.
Le projet de loi de finance pour 2018 doit encore être examiné par l'Assemblée nationale avant son adoption définitive.
(Site de la Fevad, décembre 2017)

INTERNATIONAL

USA / Données personnelles - La FTC publie un guide pour faciliter la conformité à la loi COPPA
Aux Etats-Unis, la Federal Trade Commission (FTC) a publié un guide afin de faciliter la conformité des services en ligne avec la loi sur la protection de la vie privée des enfants en ligne (Children's Online Privacy Protection Act - COPPA). Le guide est organisé en 6 étapes permettant aux organismes de se mettre en conformité avec les dispositions de la loi :

- Comment déterminer si votre société exploite un site web ou un service en ligne qui collecte des données personnelles d'enfants de moins de 13 ans ?
- Votre société a t-elle mis en ligne une politique de la vie privée adaptée ?
- Votre société informe-t-elle les parents directement de manière adaptée avant de collecter des données personnelles d'enfants de moins de 13 ans ?
- Comment recueillir un "consentement parental vérifiable" avant la collecte de données personnelles d'enfants de moins de 13 ans ?
- Votre société a-t-elle mis en place un système pour répondre aux droits des parents relatifs aux données personnelles d'enfants de moins de 13 ans ?
- Votre société a-t-elle mis en place des procédures raisonnables pour protéger la sécurité des données personnelles d'enfants ?

Le guide ne se limite pas aux sites web et prend également en compte les données collectées par l'intermédiaire des objets et jouets connectés.

(Compliance with COPPA: So easy, even a kid can do it, in Technology Law Dispatch, 5 juillet 2017)

USA / Internet – Quelles conséquences sur la fin de la neutralité du Net aux Etats-Unis ?

Le 14 décembre, la Federal Communications Commission (FCC) a voté la suppression des règles de neutralité du Net. Ce principe fondateur d'internet signifie que tous les contenus mis en ligne sont traités de la même manière, sans discrimination en termes de vitesse, et donc, de coût.

La fin de ce principe permettra aux FAI américains de proposer des tarifs variables en fonction de la rapidité du trafic internet souhaité par le client. Nombre d'entreprises devront redéfinir le mode de développement de leurs applications mobiles et leur manière d'héberger les contenus, notamment dans le cloud.

Aux États-Unis, associations et chefs d'entreprises craignent qu'une fois la suppression de ce principe entérinée, les FAI réservent un traitement préférentiel à certains services de streaming ou modulent les abonnements à internet en fonction de la rapidité d'accès aux contenus.

Selon plusieurs analystes américains, les applications d'entreprise, notamment les applications mobiles dans le cloud, pourraient être ralenties au même titre qu'un service de streaming vidéo comme Netflix. Les sociétés qui hébergent des applications en interne pourraient également modifier leurs règles d'utilisation, car les applications fréquemment utilisées, notamment celles concernant la mobilité d'entreprise, sont accessibles par internet.

En France, concernant les infrastructures, Stéphane Richard, PDG d'Orange, a déclaré début décembre que la fin de l'abandon de la neutralité du Net serait une « obligation » avec l'avènement de la 5G. L'objectif serait de peser sur l'Autorité de régulation des communications électroniques et des postes (Arcep), pour vendre des forfaits plus chers à certains types de clients afin de pouvoir moduler les flux de données, certains flux pouvant ainsi être optimisés pour le débit et d'autres pour la latence afin de répondre aux besoins des voitures connectées ou des opérations médicales à distance par exemple. Or, pour rappel, en France, la loi pour une République numérique du 7 octobre 2016, a renforcé les pouvoirs de l'Arcep, et rappelé le principe de neutralité de l'internet. L'Arcep a désormais la charge de faire respecter ce principe par les opérateurs.

(source IDG, décembre 2017 ; Les Etats-Unis abrogent la neutralité du Net, un principe fondateur d'Internet, in Le Monde, 14 décembre 2017 ; art. L.32-1 et L.33-1 du CPCE)

PUBLICATIONS

Vous trouverez sur le Blog du Cabinet toutes nos dernières publications :

- Pourquoi être concerné par le RGPD si votre entreprise n'est pas localisée dans l'UE ?
- Sécurité des données personnelles : vers la généralisation de la procédure de notification des incidents de sécurité
- Après le Parlement européen, le CESE publie un avis sur l'intelligence artificielle (IA)
- Plateformes en ligne : le Parlement européen pour une évolution de leur régime de responsabilité
- Entrée en application du RGPD en mai 2018 : comment organiser votre mise en conformité au règlement européen ?

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