LA LETTRE DU CABINET
TECHNOLOGIES DE L'INFORMATION

EDITO

Nous avons le plaisir de vous adresser le vingtième numéro de notre Newsletter.

Cette lettre est organisée autour des thématiques suivantes : un flash sur les opérations de mise en conformité au règlement général européen sur la protection des données (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, la robotique, et le droit des affaires. Nous souhaitons par ce moyen vous informer des derniers développements du droit des technologies de l'information.

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 !

SOMMAIRE

ⓘ FLASH – ENTRÉE EN APPLICATION DU RGPD EN MAI 2018 : COMMENT ORGANISER VOTRE MISE EN CONFORMITÉ AU RÈGLEMENT EUROPÉEN ?

Le règlement général européen sur la protection des données (RGPD) entrera en application dans moins d'un an, le 25 mai 2018. 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. Pour rappel, 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…

La CNIL a publié un plan pour aider les organismes à se préparer à la mise en conformité au RGPD. Celui-ci se décline en six étapes, comme suit :

- *Etape 1 : désigner une personne en charge de piloter la mise en conformité*

Compte tenu de la complexité de la mise en oeuvre de la conformité au RGPD, une personne doit être désignée pour piloter cette phase. Cette personne, interne à l'entreprise, futur délégué à la protection des données (DPD ou DPO) ou consultant externe, exercera une mission d'information, de conseil et de contrôle en interne et permettra d'organiser les actions à mener ;

- *Etape 2 : cartographier les traitements de données personnelles*

Pour mesurer l'impact du règlement européen sur la protection des données traitées par l'entreprise, les traitements réalisés doivent être recensés dans un registre ;

- *Etape 3 : prioriser les actions à mener*

Sur la base des traitements recensés, les actions de conformité à mettre en oeuvre pourront être identifiées et classées par ordre de priorité, au regard des risques des traitements réalisés, sur les droits et les libertés des personnes concernées ;

- *Etape 4 : gérer les risques*

Si des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées ont été identifiés, une analyse d'impact sur la protection des données (DPIA) devra être réalisée pour chacun de ces traitements. A noter que des lignes directrices sur les analyses d'impact ont été publiées par le groupe du G29 ;

- *Etape 5 : organiser les processus internes*

Des procédures internes devront être prévues pour assurer un haut niveau de protection des données personnelles ;

- *Etape 6 : documenter la conformité*

Le RGPD prévoit une nouvelle notion relative à la responsabilité des responsables de traitement en matière de conformité ("accountability"). Pour démontrer la conformité de l'entreprise au règlement, il conviendra de constituer et regrouper la documentation nécessaire.

INFORMATIQUE

JURISPRUDENCE

Contrat "clés en main" – Fin de l'affaire IBM / MAIF avec la condamnation définitive d'IBM à plus de 6,6 millions d'euros

Dans un arrêt du 29 mars 2017, la Cour de cassation a confirmé l'arrêt de la Cour d'appel de Bordeaux du 29 janvier 2015, ordonnant la résolution du contrat d'intégration conclu en 2004 entre la

société IBM France et la MAIF, aux torts d'IBM et sa condamnation à plus de 6,6 millions d'euros. Cette procédure arrive à son terme, clôturant une affaire ayant duré presque 10 ans.
Pour rappel la MAIF avait conclu avec IBM un contrat d'intégration pour un prix ferme et forfaitaire de 7 millions d'euros, aux termes duquel IBM s'engageait notamment à respecter le calendrier défini. Compte tenu des retards accumulés, des avenants successifs redéfinissant le périmètre et le coût du projet (3,5 puis 15 millions d'euros supplémentaires) ont dû être signés. Constatant l'impossibilité pour le prestataire de terminer le projet, la MAIF a assigné IBM.
Dans sa décision du 29 janvier 2015, la Cour d'appel de Bordeaux a rejeté la demande en nullité de la MAIF pour dol mais a retenu la responsabilité de la société IBM et a prononcé la résolution du contrat d'intégration aux torts de cette dernière. Selon la Cour, IBM a commis une faute en prévoyant un planning sans élasticité, assortie d'un forfait. « *La prévision d'un planning sans élasticité pour une opération de cette envergure, et son incidence sur le calcul du forfait retenu, présentent un caractère d'autant plus fautif qu'elles émanent d'un distributeur de produits informatiques qui rappelle lui-même qu'il est de renommée internationale, ce qui pouvait faire attendre de lui une appréciation plus juste des aléas inhérents à l'opération mise en place, et par suite aux délais de sa réalisation et au prix des prestations qu'il s'était engagé à fournir. »* Aussi, selon la Cour, ses fautes sont directement à l'origine de l'échec du projet, dont la gravité et les conséquences justifient la résolution du contrat aux torts d'IBM et sa condamnation à plus de 6.6M€. *(C. cass., ch. com., 29 mars 2017, IBM France et BNP Paribas Factor / Mutuelle Assurance des Instituteurs de France ; CA Bordeaux, 1e ch. civ., sect.B, 29 jan. 2015, IBM France et BNP Paribas Factor / Mutuelle Assurance des Instituteurs de France)*

INTERNET

RÉGLEMENTATION

Neutralité du Net – L'Arcep précise son action
La neutralité de l'internet vise à garantir l'égalité de traitement de tous les flux d'information sur internet afin que ceux-ci ne soient ni bloqués, ni dégradés, ni favorisés par les opérateurs de télécommunications ou par les fournisseurs de services.
La loi pour une République numérique, adoptée le 7 octobre 2016, a renforcé les pouvoirs de l'Autorité de régulation des communications électroniques et des postes (Arcep), et rappelé le principe de neutralité de l'internet. L'Arcep a désormais la charge de faire respecter ce principe par les opérateurs.
Fin mai 2017, Sébastien Soriano, président de l'Arcep, a détaillé un plan pour garantir que les opérateurs respectent leurs obligations en matière d'équité de traitement et de non-discrimination du trafic internet. L'Arcep dispose désormais de pouvoirs d'enquête et de sanction. Si un opérateur télécom est soupçonné de favoriser certains services, sites ou contenus sur internet, l'Autorité peut alors mener une investigation et des perquisitions et sanctionner l'opérateur fautif.
La neutralité du net est menacée en partie par les opérateurs télécoms, puisque tous les flux de données transitent par leurs tuyaux, mais également par les « géants » du Net (Google, Apple, Facebook, Amazon - GAFA). Or, l'Arcep n'a aucun pouvoir pour réguler ces plateformes, son rôle étant limité aux opérateurs télécoms traditionnels. *(« Télécoms, comment l'Arcep veut garantir la neutralité du Net », in La Tribune 30 mai 2017 ; et voir rapport de l'Arcep « L'état de l'internet en France » édition 2017 ; Loi n°2016-1321 du 7 octobre 2016 pour une République numérique et article L32-4 du CPCE)*

Numérique - Le CNNum publie un manifeste pour une politique publique numérique
Le Conseil national du numérique (CNNum), créé en 2011, a notamment pour mission de rendre des avis et des recommandations sur toute question relative à l'impact du numérique sur la société et sur l'économie. Fin mai 2017, 70 personnalités du numérique (actuels et anciens membres du CNNum) ont signé un manifeste pour interpeller l'exécutif sur l'urgence de déployer une politique publique pour accompagner la transformation numérique en France. Le CNNum estime pouvoir contribuer à la construction de cette politique et renforcer son impact au niveau européen.
Ce manifeste comprend huit sujets :

- Préfigurer une agence européenne pour la confiance numérique chargée d'évaluer la loyauté des plateformes ;
- Peser sur les décisions européennes en matière de partage et de circulation des données ;
- Préserver un modèle démocratique ouvert et respectueux des libertés en ligne dans un monde instable ;
- Penser la coexistence entre l'intelligence artificielle des machines et l'intelligence humaine ;
- Développer une politique d'inclusion par le numérique ;

- Enclencher une nouvelle phase de la transformation numérique de l'éducation et de la formation tout au long de la vie ;
- Soutenir la transformation numérique des PME françaises ; et
- Mettre la transformation numérique au service de la transition écologique.

Selon le CNNum, ce manifeste a vocation à être vivant et à évoluer avec le temps. Ainsi, un large événement réunissant plusieurs représentants de l'écosystème numérique devrait être organisé dans les semaines à venir autour des questions de transformation numérique du pays. *(Manifeste du Conseil national du numérique, mai 2017)*

Plateformes en ligne – Le Parlement européen vote une résolution en faveur de la responsabilisation des plateformes en ligne

Répondant à une Communication de la Commission européenne du 25 mai 2016, le Parlement européen a voté, le 15 juin dernier, une résolution dans laquelle les députés européens se sont prononcés en faveur de la responsabilisation des plateformes en ligne concernant le respect du droit d'auteur, la lutte contre les contenus illégaux, et la protection des mineurs et des consommateurs.

Les euro-députés constatent tout d'abord la difficulté de donner une définition unique de la notion de plateforme en ligne « *qui soit juridiquement pertinente et à l'épreuve du temps, compte tenu de facteurs tels que la grande variété des plateformes en ligne et de leurs domaines d'activités ou encore l'évolution rapide de l'environnement numérique à l'échelle mondiale* ». Ils relèvent par ailleurs les caractéristiques communes existant sur les plateformes, telles que par exemple, la possibilité de mettre en relation différents types d'utilisateurs, d'offrir des services en ligne adaptés aux préférences des utilisateurs et fondés sur des données fournies par les utilisateurs, de classer ou de référencer des contenus, notamment au moyen d'algorithmes, etc.

Le développement durable et la confiance des consommateurs dans les plateformes en ligne nécessite un environnement réglementaire « *efficace et attrayant* ». Cependant, les euro-députés proposent de préciser les obligations des intermédiaires, notamment en responsabilisant les plateformes qui ne jouent pas un rôle neutre au sens de la directive du 8 juin 2000 sur le commerce électronique, qui ne pourraient plus bénéficier du régime de responsabilité aménagé. A cette fin, les euro-députés demandent à la Commission de formuler « *des orientations sur la mise en œuvre du cadre de responsabilité des intermédiaires afin de permettre aux plateformes en ligne de respecter leurs obligations ainsi que les règles relatives à la responsabilité (...)* », notamment en clarifiant les procédures de notification et de retrait de contenus et en présentant des orientations sur les mesures volontaires de lutte contre ces contenus.

L'évolution de la responsabilité des plateformes est une demande importante du Parlement notamment pour les industries culturelles et créatives, avec un renforcement des mesures de lutte contre les contenus en ligne illégaux et dangereux – une référence étant faite à la proposition de directive SMA (services de médias audiovisuels) et aux mesures pour les plateformes de partage de vidéos concernant la protection des mineurs et le retrait des contenus associés à des discours haineux.

Par ailleurs, constatant que bien que l'on n'ait jamais autant consommé de contenus issus de la création, par l'intermédiaire de plateformes de mise à disposition de contenu par les utilisateurs et les services d'agrégation de contenus, les secteurs de la création ne bénéficient pas d'une augmentation de leurs revenus proportionnée à cette augmentation de la consommation. Alors que plusieurs textes européens sont en cours d'examen au Parlement, les euro-députés souhaitent un renforcement de la sécurité juridique et du « *respect envers les titulaires de droits ».* Selon les euro-députés, les plateformes qui hébergent un volume important d'oeuvres protégées, mises à la disposition du public, devraient conclure des accords de licence avec les titulaires de droits correspondants, (à moins qu'elles ne soient pas actives et qu'elles relèvent du régime de responsabilité prévu à l'article 14 de la directive de juin 2000), en vue de partager avec les auteurs, créateurs et titulaires de droits correspondants une juste part des bénéfices engendrés.

Le Parlement demande enfin à la Commission européenne de mener une enquête sur l'exploitation des algorithmes et de créer des conditions de concurrence équitables pour des services en ligne et hors ligne comparables.

A noter qu'une résolution n'est pas un acte réglementaire contraignant. Les résolutions ne créent pas d'obligations juridiques mais ont une valeur politique et indicative pouvant servir de référence pour clarifier un texte imprécis par exemple. *(Résolution du Parlement européen du 15 juin 2017 sur "Les plateformes en ligne et le marché unique numérique" et Communication de la Commission du 25 mai 2016 sur "Les plateformes en ligne et le marché unique numérique – Perspectives et défis pour l'Europe")*

JURISPRUDENCE

Internet - Déréférencement de photos publiées sur internet sur le fondement de l'atteinte à la vie privée

Par une ordonnance de référé rendue le 12 mai 2017, le Tribunal de grande instance de Paris a fait droit aux demandes de déréférencement, sur le moteur de recherche Google, de liens renvoyant vers des photos violant le droit à la vie privée, principe protégé par l'article 9 du code civil.

En l'espèce, une ex-mannequin avait constaté la publication de photos d'elle sur différents sites web sans son accord. La demanderesse justifiait d'un intérêt légitime à voir le déréférencement ordonné, s'agissant de clichés à connotation érotique, publiés sans autorisation, et alors même qu'elle n'exerce plus la profession de mannequin.

La mesure de déréférencement est cependant limitée à l'extension française du moteur de recherche. En effet, le droit à l'image diffère suivant les juridictions, contrairement au droit à l'oubli. *(TGI de Paris, ordonnance de référé, 12 mai 2017, Mme X. / Google France et Google Inc.)*

Concurrence déloyale - Indemnisation d'un site victime de concurrence déloyale par un concurrent

Dans un arrêt du 7 mars 2017, la Cour d'appel de Paris a confirmé la condamnation en première instance de la société Concepson, éditeur d'un site ayant copié servilement le site de son concurrent, la société Sound Strategy.

L'un des associés de la société Sound Strategy, qui édite le site studio-lowcost.com, est actionnaire de la société Concepson, qui a créé un site concurrent. Estimant que la société Concepson s'était placée dans le sillage de son site, la société Sound Strategy a assigné Concepson pour concurrence déloyale et parasitisme. Le tribunal de commerce de Paris lui avait donné gain de cause et alloué 5.000€ de dommages-intérêts. La cour d'appel de Paris a confirmé cette décision. Selon les juges, Concepson s'est inspirée de l'ensemble de la valeur économique de Sound Strategy *« en créant un site internet très similaire au sien, notamment dans le cheminement des commandes, la structure des écrans, le choix des messages, le recours à la voix d'acteurs, le mode de paiement et la livraison »*.

Cependant, la cour n'a pas suivi Sound Strategy sur l'évaluation du préjudice. Alors que celle-ci demandait 73.000€ de réparation au titre du préjudice économique et 49.822€ au titre de sa perte de marge brute, la cour a limité le préjudice économique à 5.000€, rappelant que selon les règles du droit commun de la responsabilité civile délictuelle, le préjudice doit être réparé dans son intégralité, mais sans excéder le montant de ce préjudice. Concernant la perte de marge brute, la cour a constaté que Sound Strategy n'avait justifié aucune baisse de chiffre d'affaires à compter de la mise en ligne du site concurrent. La cour alloue enfin 5.000€ de dommages-intérêts à Sound Strategy au titre du préjudice moral, car « *par cette copie quasi-servile du site internet de la Sarl Sound Strategy, la Sas Concepson a dévalorisé la valeur et l'intérêt de ce site par sa banalisation et lui a fait perdre sa visibilité sur internet, causant à cette société un préjudice moral* ». *(CA Paris, Pôle 5 ch.1, 7 mars 2017, Sound Strategy / Concepson)*

PROTECTION DES DONNÉES PERSONNELLES

RÉGLEMENTATION

RGPD – Lignes directrices adoptées par le G29 au 30 juin 2017

Les autorités de contrôle des Etats-membres (CNIL européennes), réunies au sein du G29 ont publié plusieurs lignes directrices pour accompagner les organismes dans leurs travaux préparatoires de mise en conformité au RGPD. Fin juin 2017, les lignes directrices suivantes étaient publiées :

- *Lignes directrices sur les analyses d'impact relatives à la protection des données*

La notion d'analyse d'impact relative à la protection des données (Data Protection Impact Assessment (DPIA), définie à l'article 35 du RGPD, est l'un des mécanismes prévus dans le cadre de la notion de responsabilité ("accountabilty"), permettant aux responsables de traitement de démontrer leur conformité au règlement. L'analyse d'impact a pour objet de décrire le traitement envisagé, évaluer la nécessité et la proportionnalité du traitement, et doit permettre de gérer les risques sur les droits et libertés des individus, générés par ce traitement de données.

Le non-respect de l'obligation de réaliser une analyse d'impact est passible, pour l'organisme fautif, d'une amende administrative pouvant s'élever à 10 millions d'euros ou 2% de son chiffre d'affaires mondial de l'année précédente.

- *Lignes directrices relatives au délégué à la protection des données*

Dans le cadre de l'obligation générale de conformité au RGPD, certains organismes devront nommer un délégué à la protection des données (DPD ou DPO - data protection officer). Le DPO permet aux

organismes d'assurer leur conformité au règlement européen (fonctions d'audit, de relais entre les différents départements de l'entreprise, avec les autorités de contrôle, et avec les personnes concernées).

- *Lignes directrices sur le droit à la portabilité des données*

Le droit à la portabilité des données, prévu à l'article 20 du règlement européen, permet aux personnes concernées de recevoir les données fournies au responsable de traitement, dans un format structuré et lisible par la machine et de transmettre ces données à un nouveau responsable de traitement.

- *Lignes directrices sur l'autorité du chef de file*

Ces lignes directrices permettent d'identifier l'autorité de contrôle chef de file compétente pour les traitements de données transfrontaliers, notamment lorsque le lieu de l'établissement principal du responsable de traitement est différent de son siège européen, lorsque plusieurs sociétés sont concernées au sein d'un groupe, ou lorsqu'il y a plusieurs responsables de traitement conjoints. La situation des sous-traitants est également abordée.

D'autres lignes directrices sont en cours d'élaboration : lignes directrices sur la certification, concernant la notification de violations de données personnelles, sur le consentement des personnes, enfin sur le profilage*. (Lignes directrices disponibles, en anglais, sur le site de la CNIL : Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 ; Guidelines on Data Protection Officers ("DPOs") ; Guidelines on the right to data portability ; Guidelines for identifying a controller or processor's lead supervisory authority)*

E-privacy – La proposition de règlement e-privacy continue à être débattue

La Commission européenne a publié une proposition de règlement de protection de la vie privée et des communications électroniques le 10 janvier 2017. Ce texte (proposition de règlement « e-privacy ») viendrait abroger la directive du 12 juillet 2002 sur la protection de la vie privée dans le secteur des communications électroniques (2002/58) et compléterait le RGPD. L'objectif de la Commission est que ces deux textes entrent en application à la même date, soit le 25 mai 2018. Or, la proposition de règlement e-privacy suscite encore de nombreux débats et réactions.

La proposition de règlement « e-privacy » est un texte au champ plus restreint que le RGPD. Il concerne au premier chef les "fournisseurs de services de communications électroniques" et les utilisateurs de ces services. Ces derniers peuvent être des personnes physiques, mais également des personnes morales.

Les principales dispositions de la proposition de règlement e-privacy concernent les cookies et les règles applicables au consentement des internautes. D'une manière générale, le consentement des utilisateurs concernant les cookies interviendrait lors de l'installation d'un navigateur ou d'un nouveau logiciel, et ce afin d'éviter que les utilisateurs aient à donner leur accord ou refuser les cookies sur chaque site qu'ils visitent. Or, en l'état actuel, ce texte est considéré comme trop flou. En effet, compte tenu des différentes catégories de cookies utilisées sur le web, il est difficile pour les professionnels des médias en ligne de savoir quels types de cookies seront effectivement concernés par ce consentement global en amont des sites web.

1 - Plusieurs groupes de médias européens demandent la révision du projet de règlement ePrivacy

Ces incertitudes, ainsi que les risques potentiels posés au marché de la publicité en ligne ont amené les dirigeants de plusieurs quotidiens européens à adresser une lettre ouverte au Parlement européen et au Conseil le 29 mai dernier. Parmi les signataires, figurent pour la France Le Parisien, Les Echos, L'Equipe, Le Figaro, Le Monde, Libération et La Croix. Selon les sites de médias, « *90% de l'accès à internet sur le territoire européen est contrôlé par quatre entreprises seulement : Google, Apple, Microsoft et* Mozilla ». Le nouveau règlement aboutirait à « *renforcer l'asymétrie du rapport entre les éditeurs de presse et les portails numériques mondiaux* ». Sous couvert de protéger la vie privée des internautes, les éditeurs de sites web ne pourraient plus déployer de stratégie « data » et publicitaire efficace, risquant d'impacter les stratégies de ciblage par exemple.

2 - Incertitude sur la date d'entrée en application du règlement e-privacy

Dans un rapport du 19 mai 2017, le Conseil de l'Europe a déclaré que la proposition de règlement e-privacy ne pourra entrer en application avec le RGPD, le 25 mai 2018. La directive e-privacy de 2002 resterait donc applicable.

Les règles du futur règlement e-privacy devront être cohérentes par rapport aux dispositions du RGPD. Les principales questions restant à examiner concernent les dispositions communes aux deux textes, et les contradictions éventuelles du règlement e-privacy avec le RGPD et d'autres textes communautaires ; les conséquences d'une extension de l'application des dispositions du règlement e-privacy aux services de communication OTT (Whatsapp, Skype, etc.) ; et les conséquences d'un

système de consentement global via les navigateurs et les impacts sur l'activité des sociétés de publicité en ligne.
Par ailleurs, les membres du G29 ont rendu un avis sur la proposition de règlement e-privacy le 4 avril dernier. Celui-ci a notamment souligné le fait que le règlement e-privacy baisserait le niveau de protection défini dans le RGPD concernant i) la localisation (tracking) des équipements des utilisateurs, ii) les conditions selon lesquelles l'analyse des contenus et des metadata est autorisée, iii) la manière dont les fonctionnalités sont déterminées par défaut sur les équipements et, iv) les murs de suivi (tracking).

3 - Publication par le Parlement européen d'une étude sur la proposition de règlement e-privacy

Enfin, une étude réalisée à la demande de la direction des droits des citoyens et des affaires constitutionnelles du Parlement européen, ayant pour objet l'évaluation de la proposition de règlement e-privacy, a été publiée en mai 2017. Il ressort de cette étude que la proposition de règlement serait en deçà du RGPD en matière de protection des données.
Les institutions européennes devront donc porter une attention particulière à quatre domaines, identifiés comme n'apportant pas une protection suffisante à la confidentialité des communications, à savoir : la géolocalisation, le paramétrage par défaut des navigateurs internet, les « murs de cookies », et la confidentialité des communications.
Le texte de la proposition de règlement e-privacy n'est donc pas encore arrêté. Compte tenu des questions soulevées, ce texte va probablement continuer à être débattu pendant les mois qui viennent, et son entrée en application à la date du RGPD n'est pas assurée.
(Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE ; et voir notamment, Journal du Net, 29 mai 2017 ; "Still no clarity on data protection on websites: EU ePrivacy Regulation will not come into force by May 2018", in Technology Law Dispatch, 23 mai 2017 ; Directorate General for internal policies - Citizens' rights and constitutional affairs : "An assessment of the Commission's proposal on privacy and electronic communications", mai 2017)

JURISPRUDENCE

Loi Informatique et Libertés - La CNIL prononce une amende de 15.000€ à l'encontre de la société Allocab

En 2015, la société Allocab (service en ligne de transport de personnes) a fait l'objet d'un contrôle sur place par les agents de la CNIL, à la suite d'une plainte d'un client. Lors de ce contrôle, la CNIL a relevé plusieurs manquements à la loi Informatique et Libertés.
Le 10 novembre 2015, une mise en demeure était adressée à la société, lui enjoignant notamment de définir une durée de conservation des données personnelles des clients, de ne pas conserver les données relatives aux cryptogrammes des cartes bancaires au-delà du temps nécessaire à la réalisation de la transaction, d'effacer les données des clients ayant demandé la suppression de leurs comptes, et de prendre toute mesure nécessaire pour garantir la sécurité et la confidentialité des données des utilisateurs du site.
La société Allocab a tardé à répondre aux demandes de la Présidente de la CNIL et n'a pas mis en oeuvre plusieurs des mesures de correction annoncées.
La formation restreinte de la CNIL, saisie de ce dossier, a estimé que les manquements à l'obligation de définir et de respecter une durée de conservation proportionnée à la finalité du traitement et d'assurer la sécurité et la confidentialité des données ont persisté au-delà de l'échéance du délai de mise en conformité. Le 13 avril 2017, la formation restreinte, prenant en compte la cessation des manquements à cette date, a décidé de prononcer une sanction d'un montant de 15.000 euros.
(Délibération n°SAN 2017-002 du 13 avril 2017)

Loi Informatique et Libertés - Facebook sanctionné par la CNIL pour manquements à la loi

Le 27 avril 2017, la formation restreinte de la CNIL a prononcé une sanction de 150.000€, rendue publique, à l'encontre des sociétés Facebook Inc. et Facebook Ireland Ltd pour plusieurs manquements à la loi Informatique et Libertés suite à la modification de la politique d'utilisation des données de Facebook en 2015.
En 2015, la CNIL a procédé à des contrôles sur place, sur pièces et en ligne afin de vérifier la conformité du réseau social à la loi Informatique et Libertés. Ces contrôles ont permis de constater plusieurs manquements à la loi, dont le fait que Facebook procédait à la combinaison massive des données personnelles des internautes à des fins de ciblage publicitaire et traçait à leur insu les internautes, avec ou sans compte Facebook, sur des sites tiers via un cookie « datr ».

Le 26 janvier 2016, les sociétés Facebook Inc. et Facebook Ireland Ltd ont été mises en demeure de se conformer à la loi Informatique et Libertés. En l'absence de mise en conformité dans les délais impartis, un rapporteur a été désigné afin que soit engagée une procédure de sanction à leur encontre.

Concernant la combinaison de données des utilisateurs de Facebook, le traitement est réalisé en l'absence de base légale. En effet, si les utilisateurs disposent de moyens pour maîtriser l'affichage de la publicité ciblée, ils ne consentent pas à la combinaison massive de leurs données et ne peuvent s'y opposer, que ce soit lors de la création de leur compte ou a posteriori.

Concernant la collecte des données de navigation des internautes via le cookie « datr », l'information dispensée via le bandeau relatif aux cookies est imprécise. Cette mention ne fait qu'indiquer que des informations sont collectées « (*…) sur et en dehors de Facebook via les cookies »,* ce qui ne permet pas aux internautes d'être clairement informés et de comprendre que leurs données sont systématiquement collectées dès lors qu'ils naviguent sur un site tiers comportant un module social. Cette collecte massive de données effectuée via le cookie « datr » est déloyale en l'absence d'information claire et précise.

Sur les autres manquements, la formation restreinte considère que les sociétés Facebook ne délivrent aucune information immédiate aux internautes sur leurs droits et sur l'utilisation qui sera faite de leurs données notamment sur le formulaire d'inscription au service ; elles ne recueillent pas le consentement exprès des internautes lorsqu'ils renseignent des données sensibles dans leurs profils (opinions politiques, religieuses ou orientation sexuelle) ; en renvoyant au paramétrage du navigateur, les sociétés ne permettent pas aux utilisateurs de s'opposer valablement aux cookies déposés sur leur équipement terminal ; enfin, les sociétés ne démontrent pas en quoi la conservation de l'intégralité des adresses IP des internautes pendant toute la durée de vie de leur compte est nécessaire.

En conséquence, la formation restreinte de la CNIL a décidé de prononcer une sanction de 150.000 € rendue publique à l'encontre des sociétés Facebook Inc. et Facebook Ireland Ltd.

Des procédures diligentées par les autorités de contrôle de Belgique, d'Allemagne (Land de Hambourg), d'Espagne et des Pays-Bas sont également en cours. *(Délibération n°SAN 2017-006 du 27 avril 2017 prononçant une sanction pécuniaire à l'encontre des sociétés Facebook Inc. et Facebook Ireland)*

Vidéosurveillance – Un commerçant sanctionné pour diffusion d'images issues d'un système de viodéoprotection non autorisé

Le 30 mai 2017, le TGI de Paris a condamné le responsable d'un restaurant attaqué lors de la série d'attentats à Paris le 13 novembre 2015, pour avoir utilisé un système de vidéoprotection non autorisé, et vendu des images enregistrées par ce dispositif à un quotidien britannique qui les a diffusées en ligne.

Trois des victimes de l'attentat se sont reconnues sur ces images. Après avoir demandé, en vain, au quotidien Daily Mail de les retirer, elles ont porté plainte pour violation de l'article L.254-1 du code de la sécurité intérieure relatif aux systèmes de vidéoprotection, de l'article 321-1 du code pénal pour recel et de l'article 226-1 du même code pour la captation et l'enregistrement d'images portant atteinte à l'intimité de la vie privée.

Le responsable de l'établissement avait installé un système de vidéoprotection sans autorisation préfectorale, contrairement aux dispositions de l'article L.252-2 du code de la sécurité intérieure, et alors que le prévenu avait été informé de ses obligations légales par le prestataire du service de vidéoprotection. Par ailleurs, le code de la sécurité intérieure impose d'habiliter une personne à accéder au système. Or, le prévenu a donné accès à des personnes non habilitées, qui ont pu récupérer les images pour les revendre au quotidien britannique. Pour les juges, les faits reprochés au responsable du restaurant *« présentent un caractère d'une incontestable gravité, l'intéressé n'ayant, notamment, pas hésité à monnayer âprement une vidéo relative à un événement particulièrement tragique ayant profondément affecté non seulement les victimes directes mais également la communauté nationale et internationale, et à porter atteinte de manière durable à l'intégrité psychique d'hommes et de femmes déjà durement éprouvés par ce drame ».*

Le prévenu a été condamné à une peine d'amende de 10.000€. Les deux personnes non habilitées ayant accédé au dispositif ont été condamnées respectivement à 5.000€ et 1.500€ d'amende. Les prévenus doivent, en outre, verser solidairement 5.000€ de dommages-intérêts aux parties civiles pour préjudice moral, et 1.000€ au titre de l'article 475-1 du code de procédure pénale. *(TGI de Paris, 17e ch. corr., 30 mai 2017 M. D., Mme C., M. I., Mme X. et M. Y. / M. M., M. S. et M. H.)*

PROPRIÉTÉ INTELLECTUELLE

JURISPRUDENCE

Contrefaçon – La Cour de cassation confirme le mode de calcul du préjudice subi pour contrefaçon du logiciel Windows

Dans un arrêt du 19 avril 2017, la Cour de cassation a confirmé la décision de la Cour d'appel de Rennes du 23 septembre 2016, qui avait forfaitairement évalué le préjudice matériel de la société Microsoft à la somme de 819.855,75 euros, calculé sur la base du prix des licences OEM Windows (Original Equipment Manufacturer).

Dans cette affaire, le prévenu a été condamné pour avoir contrefait et commercialisé des logiciels OEM, concédés par la société Microsoft à des constructeurs pour être installés sur des ordinateurs neufs. Les logiciels sous licence OEM ne sont pas transférables sur d'autres ordinateurs, contrairement aux logiciels sous licence FPP (Full Package Product), plus chers de 25% mais transférables. Microsoft avait calculé son préjudice sur la base des licences FPP et contesté la décision de la cour d'appel.

La Cour de cassation a décidé que, dès lors que l'indemnisation n'était pas inférieure aux droits qui auraient été dus si le prévenu avait demandé l'autorisation de commercialiser les logiciels sous licence OEM, la cour d'appel a justifié sa décision. *(C. cass., ch. crim., 19 avril 2017, M. X. / Microsoft Corporation)*

Contrefaçon – La CJUE valide le blocage des plateformes BitTorrent

Le 14 juin 2017, la Cour de justice de l'Union européenne (CJUE) a rendu un arrêt permettant le blocage de la plateforme The Pirate Bay (blocage des noms de domaine et des adresses IP de la plateforme).

Dans cette affaire intentée par la fondation néerlandaise Stichting Brein, en charge de la défense des ayants droit, à l'encontre de deux fournisseurs d'accès, la CJUE devait déterminer si une plateforme de partage peut constituer une communication au public.

Les ayants droit demandaient le blocage de la plateforme The Pirate Bay afin de faire cesser la diffusion illégale d'œuvres protégées par le droit d'auteur. Or, les sites de partages de fichiers torrent soutiennent qu'ils ne partagent pas les contenus car ils ne possèdent pas sur leurs serveurs de contenus illégaux à proprement parler. Ils donnent simplement le moyen de retrouver ces contenus.

La Cour a rappelé que la directive droit d'auteur du 22 mai 2001 (directive 2001/29/CE) avait instauré un niveau élevé de protection. La notion de communication au public doit donc être interprétée selon ces critères.

En référence aux jurisprudences Svensson, BestWater et GS Media, la Cour considère « *que tout acte par lequel un utilisateur donne, en pleine connaissance de cause, accès à ses clients à des œuvres protégées, est susceptible de constituer un acte de communicatio »".* En l'occurrence, par la mise à disposition et la gestion de la plateforme de partage en ligne The Pirate Bay, ses administrateurs offrent à leurs utilisateurs un accès aux œuvres concernées. Ils peuvent donc être considérés comme jouant un rôle incontournable dans la mise à disposition des œuvres en cause.

En outre, les administrateurs de la plateforme de partage en ligne procèdent à l'indexation des fichiers torrents, ce qui facilite leur localisation et le téléchargement et proposent un moteur de recherche et un index des œuvres. La Cour en conclut qu'il y a bien acte de communication.

La Cour a ensuite démontré qu'il y a communication au public, à savoir l'ensemble des utilisateurs de la plateforme, et qu'il s'agit d'un public nouveau, qui n'avait pas été pris en compte par les titulaires des droits lorsque la communication initiale avait été autorisée. Elle relève, enfin, que l'activité de la plateforme lui permettait de réaliser des recettes publicitaires considérables. *(Arrêt de la CJUE, 2é ch., Stichting Brein c. Ziggo BV et XS4All internet BV, affaire C-610/15, 14 juin 2017)*

ROBOTIQUE

RÉGLEMENTATION

Robots – Après le Parlement européen, le CESE publie un avis sur la robotique

Après les recommandations sur la robotique, émises par le Parlement européen en février dernier (voir notre dernière newsletter), le Conseil économique social et européen (CESE) vient de se prononcer sur ce sujet dans un avis publié le 31 mai 2017.

Alors que l'intelligence artificielle (IA) présente de multiples avantages dans de nombreux domaines (industrie, services, éducation, etc.), des questions se posent en matière de sécurité, de contrôle des

robots intelligents et de l'IA, mais également en matière d'éthique et de protection de la vie privée, sans oublier les impacts sur la société et l'économie.
Onze domaines ont été relevés par le CESE, pour lesquels des réponses doivent être apportées : l'éthique ; la sécurité ; la vie privée ; la transparence et l'obligation de rendre des comptes ; le travail ; l'éducation et les compétences ; l'(in)égalité et l'inclusion ; la législation et la réglementation ; la gouvernance et la démocratie ; la guerre ; la super-intelligence.
Certaines des préconisations du Conseil rejoignent celles du Parlement européen. Le CESE préconise notamment :

- l'instauration d'un code européen de déontologie pour le développement, le déploiement et l'utilisation de l'IA, afin que les systèmes d'IA demeurent, tout au long de leur processus d'exploitation, compatibles avec les principes de dignité humaine, d'intégrité, de liberté, de respect de la vie privée, de diversité culturelle et d'égalité entre hommes et femmes, ainsi qu'avec les droits fondamentaux ;
- la mise en place d'un système européen de normalisation pour la vérification, la validation et le contrôle des systèmes d'IA, fondé sur des normes de sécurité, de transparence, d'intelligibilité, d'obligation de rendre des comptes et de valeurs éthiques. Comme le Parlement, le Conseil reconnaît que la robotique doit être réglementée au niveau pan-européen, notamment pour des raisons concurrentielles sur le marché mondial.

En revanche, contrairement au Parlement européen, le Conseil se prononce contre la création d'une personnalité juridique spécifique pour les robots. Le CESE prône une approche dite « human-in-command » de l'IA, reposant sur un développement responsable, sûr et utile de l'IA, dans le cadre duquel les machines resteraient les machines, sous le contrôle permanent des humains. *(« Le CESE n'est pas favorable à la création d'une personnalité juridique pour les robots ou l'IA », in Le Monde du Droit, 14 juin 2017)*

DROIT DES AFFAIRES

JURISPRUDENCE

Concentrations - La Commission impose une amende de 110 millions € à Facebook suite à l'acquisition de WhatsApp

Le 18 mai 2017, la Commission européenne a annoncé avoir imposé une amende de 110 millions d'euros à Facebook Inc., pour avoir fourni des informations inexactes ou dénaturées au cours de l'enquête menée par ses services en 2014, préalablement à l'acquisition de la société WhatsApp par Facebook. Il s'agit de la première décision de sanction rendue par la Commission depuis l'entrée en vigueur du règlement européen de 2004 sur les concentrations.
Ce règlement de 2004 oblige les entreprises soumises à une enquête en matière de concentration à fournir des renseignements exacts et non dénaturés, pour que la Commission puisse examiner les concentrations et acquisitions en temps utile et de manière efficace.
Lorsque Facebook a notifié l'acquisition de la société WhatsApp à la Commission en 2014, Celle-ci a déclaré qu'elle ne serait pas en mesure d'établir de manière fiable la mise en correspondance automatisée entre les comptes d'utilisateurs de Facebook et ceux de WhatsApp. Or, en août 2016, WhatsApp a annoncé des mises à jour de ses conditions générales d'utilisation et de sa politique de confidentialité, y compris la possibilité d'associer les numéros de téléphone des utilisateurs de WhatsApp aux profils d'utilisateur de Facebook.
Le 20 décembre 2016, la Commission a adressé une communication de griefs à Facebook, dans laquelle elle expose ses préoccupations. Contrairement à ce qu'avait déclaré Facebook, la possibilité technique de mettre en correspondance les identités des utilisateurs de Facebook et de WhatsApp existait déjà en 2014, et les employés de Facebook étaient au courant de cette possibilité.
La sanction de la Commission n'a cependant pas d'incidence sur la décision de la Commission d'octobre 2014 d'autoriser l'opération de rachat.
Les nouvelles conditions d'utilisation de WhatsApp avaient été contestées par les autorités de protection de la vie privée européennes, le G29 ayant demandé la suspension de ce rapprochement entre les deux applications. Facebook a suspendu cette fonctionnalité en Europe fin 2016. *(« Concentrations : la Commission inflige des amendes de 110 millions EUR à Facebook pour avoir fourni des renseignements dénaturés concernant l'acquisition de WhatsApp », communiqué de presse de la Commission européenne, 18 mai 2017)*

PUBLICATIONS

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

- Gérer et protéger ses données à l'ère du numérique, un impératif de bonne gouvernance pour l'entreprise

- De la science-fiction au droit : vers un cadre juridique européen de la robotique à l'aube d'une nouvelle révolution industrielle

- Publication du décret sur la transparence de la publicité en ligne

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