Journée d'actualisation de Droit de l'internet

En partenariat avec l'Association Française des Juristes d'Entreprise (AFJE)

Vendredi 15 mars 2019

Dossier documentaire

Faculté de droit et de science politique de Montpellier

Nous tenons à remercier Madame Agnès Robin, Madame Nathalie Mallet-Poujol, d'avoir consacré temps et énergie à la réalisation de ce colloque.

Un grand merci également à Madame Anne-Emmanuelle Rousseau, Déléguée régionale de l'Association Française des Juristes d'Entreprise, partenaire de l'événement, ainsi qu'à tous les intervenants pour leur implication dans cette journée.

Merci enfin à la promotion 2018-2019 du Master 2 « Droit de la propriété Intellectuelle et TIC » pour la réalisation du dossier documentaire (Sarah Damoun, Cédric David, Arnaud Fabre, Ludmylia Gene, Inès Gueddana, Baptiste Meunier et Tomas Ornowski).

SOMMAIRE

Internet et places de marché
par Mme Agnès Robin, Maître de conférences HDR, Université de Montpellier

Proposition de règlement du Parlement Européen et du Conseil promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne, 26 avril 2018, COM(2018) 238 final

Internet et distribution
par Mme Sandrine Roose-Grenier, Maître de conférences en Droit privé, Université de Montpellier

I – Distribution sélective et plateformes en ligne
1- Paris, 8e ch., 13 juill. 2018 (n° 17/20787) *Affaire eNova Santé c/ Caudalie*
2- Autorité de la concurrence, Décision n° 18-D-23 du 24 octobre 2018, *Affaire Andreas Stihl SAS, StihlHolding AG & CO KG*

II – Concurrence et activité illicite sur des plateformes en ligne
1- Paris, 1re ch., 6 nov. 2018 (n° 17/104957), *Conseil National des barreaux c/ Demander Justice*
2- Versailles, 1re ch., 7 déc. 2018 (n° 17/05324), *Conseil National des barreaux c/ Jurisystem*

Internet et consommation
par Mme Linda Boudour, Magistrat, Tribunal de Grande Instance de Verdun

1- CJUE 25 janvier 2018, n° C-498/16 *Affaire. Schrems*
2- TGI Paris 7 août 2018, *UFC Que Choisir c/ Twitter*

Internet et données personnelles
par Me Julien Le Clainche, avocat au Barreau de Montpellier

Textes

1 - Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel, *JORF* n° 0288 du 13 décembre 2018
2 - Décret n° 2018-687 du 1er août 2018 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, *JORF* n° 0177 du 3 août 2018
3 - Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, *JORF* n° 0141 du 21 juin 2018
4 - Règlement (UE) 2016/79 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *JOUE* L 119/1 (RGDP).

Jurisprudence

I- Formalités
1- CA Paris, ch.8 1er mars 2019, *M. X./ Oxeva*

2- CJUE 5 juin 2018, C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c/ Wirtschaftsakademie Schleswig-Holstein GmbH*

II- Consentement
CE 10ème – 9ème ch. Réunie, 6 juin 2018, *Editions Croque Futur/Cnil*, n° 412589

Délibérations CNIL

I – Consentement libre, éclairé et spécifique
1- Dél. 2018-042 du 30 octobre 2018 mettant en demeure la société *Vectaury* (clôturée)
2- Dél. 2018-043 du 8 octobre 2018 mettant en demeure la société *Singlespot*
3- Dél. 2018-023 du 25 juin 2018 mettant en demeure la société *Fidzup*

II – Sécurité
1- Dél. 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société *Google LLC* (50.000.000€)
2- Dél. 2018-012 du 26 décembre 2018 prononçant une sanction pécuniaire à l'encontre de la société *Bouygues Telecom* (250.000€)
3- Dél. 2018-011 du 19 décembre 2018 prononçant une sanction pécuniaire à l'encontre de la société *Uber France SAS* (400.000€)

III – Vidéosurveillance
Dél. 2018-041 du 8 octobre 2018 mettant en demeure l'*Association « 42 »*

IV – Détournement de finalité
Dél. 2018-034 du 25 septembre 2018 mettant en demeure la société *Malakoff Médéric Mutuelle*

Internet et fraude informatique *par Me Alexandre Bories, avocat au Barreau de Montpellier*

1- Cass. com., 28 mars 2018, n° 16-20018 : *Comm. Com. Electr.*, mai 2018, com. 34, note G. Loiseau
2- CA Paris, 15 sept. 2017 : *Comm. Com. Electr.,* févr. 2018, com. 16, note E.-A. Caprioli
3- CA Paris, 14 nov. 2017 : *Revue Lamy Droit de l'immatériel*, janv. 2018/144, p. 39 et *legalis.net*
4 Cass. crim., 7 nov. 2017, n° 16-84918 : *Comm. Com. Electr.,* avr. 2018, com. 31, note E.-A. Caprioli
5- Cass. crim., 27 mars 2018, n° 17-81989 : *Comm. Com. Electr.,* juill.-août 2018, com. 59, note E.-A. Caprioli
6- Cass. crim., 16 janv. 2018, n° 16-87168 : *Comm. Com. Electr.,* avr. 2018, com. 30, note E.-A. Caprioli

Internet et relations de travail *par Me Axel Saint-Martin, avocat au Barreau de Montpellier*

1- CEDH, 5° sect. 22 févr. 2018, n° 588/13
2- Cass. soc.,13 juin 2018, n° 16-17865
3- Cass. soc.,12 sept. 2018, n° 16-11690

Proposition de règlement du Parlement européen et du Conseil promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne, 26 avril 2018, COM(2018) 238 final

La proposition de règlement de la Commission européenne vise à assurer davantage de transparence dans le fonctionnement des plateformes en ligne, et permettre une meilleure résolution des litiges

Les services d'intermédiation en ligne sont de puissants acteurs du commerce électronique. En effet, en permettant la mise en relation des consommateurs avec les entreprises, les plateformes en lignes se sont vite imposées comme incontournables au point que les entreprises utilisatrices en sont devenues dépendantes. En raison de leur position quasi-dominante sur le marché, les services d'intermédiation en ligne ont pu user « de pratiques commerciales potentiellement préjudiciables qui limitent les ventes des entreprises utilisatrices par l'intermédiaire de ces services », notamment la modification sans justification et sans préavis de leurs modalités et conditions, le manque de transparence quant au classement des biens et services des entreprises.

De même, les moteurs de recherche en ligne — autres acteurs majeurs de l'économie numérique —, posent un problème de dépendance économique du fait de leurs pratiques de classement des entreprises.

Dans ce contexte, la proposition de règlement de la Commission européenne a pour objectif de rééquilibrer les relations commerciales entre les entreprises et les plateformes.

Afin d'assurer « un environnement juridique équitable, prévisible, durable et inspirant confiance » pour les entreprises utilisatrices et les fournisseurs de services d'intermédiation en ligne et de moteurs de recherche en ligne, la proposition de règlement prévoit que :

- les fournisseurs de services d'intermédiation en ligne devront rendre leurs conditions et modalités facilement compréhensibles et accessibles, et notifier les entreprises utilisatrices de toute modification de ces conditions avec un délai de préavis raisonnable (15 jours minimum) et proportionné, sous peine de nullité ;

- en cas de résiliation ou de suspension de ses services, le fournisseur de services d'intermédiation en ligne devra informer l'entreprise concernée des motifs justifiant cette décision ;

- les fournisseurs de services d'intermédiation en ligne devront indiquer très clairement dans leurs conditions et modalités, les principaux paramètres déterminant le classement des entreprises et l'importance de ces paramètres quant aux autres paramètres. Les fournisseurs de moteurs de recherche en ligne seront tenus d'indiquer par une description facilement et publiquement accessible, les principaux paramètres déterminant le classement des entreprises. Néanmoins, les fournisseurs de services d'intermédiation en ligne et de moteurs de recherche en ligne ne seront pas tenus de divulguer des secrets d'affaires ;

- les fournisseurs de service d'intermédiation en ligne devront fournir dans leurs conditions et modalités, une description de tout traitement différencié qu'ils accorderaient ou seraient susceptibles d'accorder, en fonction des biens et services proposés aux consommateurs par ces services d'intermédiation ou par les entreprises utilisatrices ;

- les fournisseurs de service d'intermédiation en ligne devront préciser dans leurs conditions d'utilisation, les modalités d'accès aux données personnelles ou autres données pour les entreprises utilisatrices ;

- les fournisseurs de services d'intermédiation en ligne devront fournir et publier dans leurs conditions et modalités, une liste des raisons restreignant la possibilité pour les entreprises utilisatrices de proposer aux consommateurs les mêmes biens et services à des conditions différentes et par d'autres moyens que ces services d'intermédiation en ligne ;

- les fournisseurs de services d'intermédiation en ligne devront mettre à disposition des entreprises utilisatrices un service interne de traitement des plaintes facilement accessible, dès lors que ces fournisseurs de service d'intermédiation emploient plus de 50 salariés ;

- les fournisseurs de services d'intermédiation en ligne devront indiquer dans leurs conditions et modalités, un ou plusieurs médiateurs avec lesquels ils sont prêts à entrer en contact en cas de litige avec une entreprise utilisatrice, afin de parvenir à un accord. Les fournisseurs de service d'intermédiation en ligne prendront en charge au moins la moitié du coût total de la médiation ;

- les organisations et entités représentatives des entreprises utilisatrices ainsi que les organismes publics chargés de défendre les intérêts de ces entreprises auront le droit de saisir les tribunaux nationaux dans l'Union « en vue de faire cesser ou d'interdire tout manquement, de la part de fournisseurs de services d'intermédiation en ligne ou de moteurs de recherche en ligne, aux exigences » du règlement ;

- la Commission encourage les services d'intermédiation en ligne et les moteurs de recherche ainsi que les organismes et associations les représentant à mettre en place des codes de conduite visant à contribuer à une application correcte du règlement.

Références doctrinales :

- A. Robin, « Places de marché en ligne. Distinctions et définitions », *JCl. Contrats - distribution,* Fasc. à paraître, 2019.
- A. Robin, « Places de marché en ligne. Contrat de marketplace », *JCl. Contrats - distribution,* Fasc. à paraître, 2019.
- A. Robin, « Places de marché en ligne. Responsabilité », *JCl. Contrats - distribution,* Fasc. à paraître, 2019.

Internet et distribution

Mme Sandrine Roose-Grenier, Maître de conférences, Université de Montpellier

I- Distribution sélective et plateformes en ligne

1- Paris, 8e ch., 13 juill. 2018, n° 17/20787, *Affaire eNova Santé c/ Caudalie*

Les produits cosmétiques n'étant pas des produits banals du fait de l'allure et de l'image de prestige qui leur confèrent une sensation de luxe, un fournisseur de tels produits peut interdire leur vente sur des plateformes de vente en ligne tierce.

Faits. – La société Caudalie souscrit avec des pharmaciens deux types de contrats dans le cadre de son réseau de distribution sélective : l'un pour la distribution au sein de l'officine et l'autre, lié au premier, qui permet d'y ajouter la vente à distance sur internet. Ce second type de contrat exclut le recours à des plateformes tierces. S'apercevant que la société Enova Santé, éditrice de la plateforme internet *1001pharmacies.com,* commercialise ses produits sans son autorisation, la société Caudalie l'a fait assigner pour qu'il lui soit délivré injonction de cesser la commercialisation de ses produits sur son site

Par ordonnance du 31 décembre 2014, le juge des référés du tribunal de commerce de Paris a, sur le fondement de l'article 873 alinéa 1er du code de procédure civile enjoint à la société Enova Santé de cesser toute commercialisation des gammes de produits de marque Caudalie et de supprimer toute référence à ces produits sur le site internet *1001pharmacies.com* dans les 30 jours de la signification de l'ordonnance, le tout sous astreinte de 1 000 euros par jour de retard et par infraction, pendant un délai de 30 jours.

La Cour d'appel de Paris ayant considéré le 2 février 2016 qu'il n'y avait pas lieu à référé, la société Caudalie décide alors de former un pourvoi en cassation et obtient un nouveau renvoi devant la Cour d'appel.

ARRÊT (Extrait)

« (…) Il résulte de la jurisprudence de la Cour de justice de l'Union européenne (CJUE, 1ère ch., 6 décembre 2017, aff. C-230/16, Coty Germany) qu'un système de distribution sélective de produits de luxe visant, à titre principal, à préserver l'image de luxe de ces produits est conforme à cette disposition, pour autant que le choix des revendeurs s'opère en fonction de critères objectifs de caractère qualitatif, fixés d'une manière uniforme à l'égard de tous les revendeurs potentiels et appliqués de façon non discriminatoire, et que les critères définis n'aillent pas au-delà de ce qui est nécessaire.

En l'occurrence, les produits de la marque Caudalie correspondent à des produits de luxe, ainsi que l'indique la société demanderesse à la mesure d'interdiction. Le seul fait qu'il s'agisse de produits de parapharmacie n'en fait pas des produits banals, contrairement à ce qu'indique la société Enova Santé. (…) Ainsi que l'expose la CJUE au paragraphe 25 de [l'arrêt Coty], la qualité de tels produits résulte non pas uniquement de leurs caractéristiques matérielles, mais également de l'allure et de l'image de prestige qui leur confèrent une sensation de luxe et cette sensation constitue un élément essentiel desdits produits pour qu'ils soient distingués, par les consommateurs, des autres produits semblables (…)

Si le caractère objectif des critères de sélection des pharmaciens agréés n'est pas contesté, la société Enova Santé expose que l'application qu'en ferait la société Caudalie serait discriminatoire. Elle

indique à cet égard que la société Caudalie aurait agréé les chaînes de magasins Marionnaud et Beauty Success pour la vente de ses produits. Cependant, la société Caudalie justifie avoir mis fin à ses relations commerciales avec la société Marionnaud, ainsi qu'il résulte de la lettre recommandée avec demande d'avis de réception qu'elle lui a adressée le 27 février 2015 et avoir obtenu que la société Beauty Success, qui exploite le site intitulé le Club Santé, cesse également la vente de ses produits. De la même manière, la société Caudalie justifie avoir engagé les démarches pour que la société Amazon cesse de proposer ses produits à la vente. Aussi n'apparaît-il pas que le réseau de distribution sélective mis en place par la société Caudalie procède de critères discriminatoires.

Dès lors que les contrats passés entre la société Caudalie et les pharmaciens de son réseau ne restreignent pas la concurrence au sens de l'article 101, § 1, du TFUE, la question de savoir si ceux-ci peuvent bénéficier, en vertu de l'article 101, § 3, d'une exemption au titre du règlement n° 330/2010 n'a pas lieu de se poser. Au demeurant et à titre surabondant, il résulte de la jurisprudence précitée de la Cour de Luxembourg qu'une interdiction de revente en ligne par le truchement d'une plateforme telle que celle proposée par la société Enova Santé ne constitue pas une restriction caractérisée au sens du règlement d'exemption (UE) n° 330/2010.

Par ailleurs, le Conseil de la concurrence, qui s'était saisi d'office des pratiques mises en œuvre dans le secteur de la distribution des produits cosmétiques vendus sur conseil pharmaceutique et concernant des produits dits haut de gamme, au nombre desquels ceux de la société Caudalie, a rendu une décision le 8 mars 2007 aux termes de laquelle cette autorité administrative indépendante indiquait accepter les engagements pris notamment par la société Caudalie consistant en la modification de ses contrats de distribution sélective et en la rédaction d'un contrat spécifique pour la vente par internet réservée aux membres de son réseau.

Au regard de l'ensemble de ces éléments, la société Caudalie justifie de la licéité de son réseau de distribution sélective. L'atteinte qui y est portée par la société Enova Santé procède d'un trouble manifestement illicite auquel les mesures adoptées par le premier juge permettent de remédier de manière pertinente.

Il convient en conséquence de confirmer l'ordonnance entreprise et de rejeter l'ensemble des demandes de la société Enova Santé étant observé que les chefs de demande formulés dans le dispositif de ses conclusions jusqu'à la demande d'infirmation de l'ordonnance ne visent pas à la reconnaissance d'un droit mais procèdent de moyens qui n'ont pas lieu de figurer dans le dispositif des écritures. »

Références doctrinales :
- C. Maréchal, « Affaire Caudalie : les places de marché écartées de la distribution sélective », *Dalloz IP/IT* 2018 p. 645.
- L. et J. Vogel, « Interdiction du recours aux places de marché par l'arrêt Caudalie : une décision bienvenue, une consécration à parachever », *AJ contrats,* 2018, p. 435.
- A.-C. Martin, « Distribution sélective et vente en ligne : confirmation et précision de la possibilité d'interdire le recours à des plateformes tierces », *LEDICO*, oct. 2018, n° 1114, p. 3.

2- Autorité de la concurrence, Déc. n° 18-D-23 du 24 octobre 2018, *Aff. Andreas Stihl SAS, StihlHolding AG & CO KG*

Par cette décision, l'Autorité se prononce pour la première fois sur les possibilités de distribution sélective et de restrictions à la vente en ligne depuis l'arrêt Coty de la CJUE du 6 décembre 2017, qui a clarifié le cadre communautaire applicable à la distribution sélective sur internet. Cette décision a ainsi vocation à préciser le cadre applicable en France pour les différents secteurs et produits, au-delà du secteur de la motoculture.

Faits. – De 2006 à 2014, Stihl imposait dans ses contrats de distribution une obligation de « *mise en main complète de la machine, avec montage du matériel, explications de fonctionnement et précautions à prendre pour un usage dans des conditions de sécurité optimale.* » De plus, cette mise en main ne pouvait se faire que dans le point de vente ou au domicile de l'acheteur par un collaborateur de Stihl. Cela excluait *de facto* la livraison par un tiers au réseau de distribution sélective, et par conséquence toute vente à distance d'un produit Stihl ou Viking. Le Président de Stihl avait confirmé cela en déclarant lors de son audition par les services de la Direccte que « *jusqu'à la fin de l'année 2013, la vente à distance des produits STIHL VIKING était purement interdite par STIHL.* » À partir de 2014, cette interdiction avait été levée pour un petit groupe de produits seulement.

« Compte tenu de la nature des produits vendus par Stihl la mise en place d'un réseau de revendeurs agréés est légitime. Il est possible pour un fabricant de réserver la vente de ses produits à un réseau de revendeurs spécialisés pour des exigences légitimes telles que la vente de produits de haute qualité ou technicité. La nécessité de contrôler le respect de ces obligations et de préserver son image de marque peut, par ailleurs, justifier l'interdiction de la vente en ligne des produits concernés sur des plateformes tierces.

Mais les modalités de vente en ligne définies par Stihl restreignent de façon disproportionnée la concurrence. La remise en main propre exigée par Stihl n'est imposée par aucune réglementation nationale ou européenne portant sur la commercialisation des produits en cause. Seule la remise d'une notice d'utilisation dans la langue de l'acheteur avec la mention de certaines informations spécifiques pour les produits dangereux est obligatoire.

Une concurrence amoindrie au détriment des consommateurs. En imposant cette remise en main propre, Stihl a retiré tout intérêt à la vente en ligne pour les distributeurs et consommateurs, qui n'ont ainsi pas pu pleinement faire jouer la concurrence entre les distributeurs et bénéficier de prix plus intéressants (jusqu'à 10 % moins cher). Ainsi, l'Autorité de la concurrence a prononcé une sanction de 7 millions d'euros à l'encontre de Stihl et lui a enjoint de modifier ses contrats de distribution sélective afin de stipuler, en termes clairs, que les distributeurs agréés ont la possibilité de procéder à la vente en ligne de tous les produits Stihl et Viking, sans exiger une remise en main propre auprès de l'acheteur. »

Références doctrinales :
- M. Chagny, « Une interdiction d'interdire la vente en ligne à géométrie variable ; Note sous Autorité de la concurrence, décision numéro 18-D-23 du 24 octobre 2018 relative à des pratiques mises en œuvre dans le secteur de la distribution de matériel de motoculture », *RJC* n° 6, p. 477-478, novembre 2018.
- D. Bosco, « Première décision "post-Coty" de l'Autorité de la concurrence », *Contrats Concurrence Consommation*, n° 12, p. 33-34, déc. 2018.
- I. Baudu, « Distribution sélective et vente en ligne : de nouveaux éclairages apportés par l'Autorité de la concurrence », *Revue Lamy de la Concurrence*, n° 78, p. 4-5, déc. 2018.
- M. Malaurie-Vignal, « Distribution sélective – Coty : acte III », *Contrats Concurrence Consommation*, n° 1, janvier 2019, comm. 6.

II- Concurrence et activités illicites sur des plateformes en ligne

1- Paris, 1re ch., 6 nov. 2018 (n° 17/104957), *Conseil National des barreaux c/ Demander Justice*

La société Demander Justice n'effectue pas d'activité de représentation en justice réservée aux avocats, ni de consultation ou de rédaction d'actes en matière juridique. Il lui est cependant enjoint

sous astreinte de faire disparaître de son site la mention de taux de réussite pouvant induire l'internaute en erreur et l'utilisation d'un petit personnage portant les habits de juge laissant penser aux internautes qu'ils ont à faire à un site officiel.

Faits. – La société Demander Justice exploite deux sites internet intitulés www.demanderjustice.com et www.saisirprudommes.com, lesquels, moyennant rémunération, mettent à la disposition des clients, des formulaires-type de mise en demeure et permettent de saisir, sans recourir à un avocat, une juridiction de proximité, un tribunal d'instance ou un conseil des prud'hommes, selon le litige.

Le 8 décembre 2014, le Conseil national des barreaux (CNB) a fait assigner la société Demander Justice devant le tribunal de grande instance de Paris, essentiellement pour qu'elle soit condamnée sous astreinte à cesser toute activité d'assistance et de représentation en justice, de consultation juridique et de rédaction d'actes sous seing privé et à cesser l'exploitation des sites internet litigieux.

Par jugement du 11 janvier 2017, le tribunal de grande instance de Paris a débouté l'ordre des avocats au barreau de Paris de l'ensemble de ses demandes et condamné in *solidum* le Conseil national des barreaux et l'ordre des avocats à payer à la société Demander Justice la somme de 5 000 euros au titre de l'article 700 du code de procédure civile et aux entiers dépens de l'instance. L'ordre des avocats au barreau de Paris et le Conseil national des barreaux ont interjeté appel.

ARRÊT (Extrait)

« (…) Considérant que la société Demander Justice met ainsi à la disposition des internautes qui sont confrontés à un litige qu'ils ne peuvent résoudre, pour un montant et dans un domaine où le ministère d'avocat n'est pas obligatoire, un logiciel leur permettant de choisir, parmi un certain nombre de thèmes, celui qui les préoccupe pour envoyer à l'adversaire, selon le modèle proposé, une lettre de mise en demeure qui lui sera expédiée, avec la possibilité, en cas d'absence de réponse, d'adresser une déclaration de saisine de la juridiction compétente désignée par un logiciel en libre accès du ministère de la justice ;

Considérant que l'internaute justiciable, qui choisit librement et seul de déclencher le processus, (lettre recommandée puis le cas échéant saisine du tribunal), manifeste sa volonté de saisir la juridiction en appuyant sur un bouton de signature électronique (…) ;

Considérant en l'espèce [à propos de l'assistance juridique] que c'est l'internaute-justiciable qui fait seul ce travail en choisissant parmi les modèles proposés et classés celui qui convient à son cas (…) que le site Demander Justice effectue ainsi une prestation matérielle de mise à disposition d'une bibliothèque documentaire et non une assistance juridique au sens précité ; que l'envoi de la déclaration est également une prestation matérielle d'entreprise ;

Considérant que la lettre de mise en demeure n'est pas remplie par la société Demander Justice qui en fournit seulement un modèle de sorte qu'il n'est pas possible de lui faire grief, ce faisant, de rédiger un acte juridique ;

Considérant qu'en l'absence de toute activité de consultation ou de rédaction d'actes en matière juridique par la société Demander Justice, il ne peut y avoir d'activité illégale de démarchage à cette fin, ni de publicité trompeuse au sens du décret 72-785 du 25 août 1972 ;

Considérant sur les taux de réussite cités sur le site qu'ils ne reposent sur aucune étude indiquée; qu'il est effectivement impossible que les pourcentages de réussite restent inchangés au fur et à

mesure des années qui passent (…) qu'il convient non pas d'interdire le site mais d'enjoindre sous astreinte de 5 000 euros par jour de retard à la société Demander Justice de les faire disparaître de son site dans le mois de la signification de cet arrêt, sauf à en mentionner les modalités précises de calcul ;

Considérant sur l'utilisation d'un bandeau tricolore, d'un logo et d'une figurine que l'utilisation d'un petit personnage portant les habits de juge avec un habit bleu, blanc et rouge sous un bandeau ou un liseré tricolore est de nature à laisser penser aux internautes qu'ils ont à faire à un site officiel (…) ;

Considérant dès lors que sans qu'il soit nécessaire pour autant d'ordonner la fermeture du site, il sera fait interdiction à la société Demander Justice, afin d'éviter tout risque de confusion, de continuer à utiliser ensemble les trois couleurs du drapeau français, un mois après la signification de cette décision, sous astreinte de 5 000 euros par jour de retard ;

Considérant que le CNB et l'ordre des avocats devront toutefois verser, chacun, à la société Demander Justice la somme de 2 500 euros sur le fondement de l'article 700 du code de procédure civile pour les frais irrépétibles exposés en cause d'appel et supporter les dépens d'appel (…) ».

Références Doctrinales :
- L. Garnerie, « Pour Demander Justice, ni fermeture, ni drapeau tricolore », *Gaz. Pal.* 13 nov. 2018, n° 3349, p. 6.
- J.-B. Crabières, « L'avocat, les geeks et le service public », *Dalloz IP/IT*, 2019 p. 122.
- G. Loiseau, « Le monopole en réduction des avocats », *Communication Commerce électronique,* n° 1, Janv. 2019, comm. 3.

2- Versailles, 1re ch., 7 déc. 2018 (n° 17/05324), *Conseil National des barreaux c/ Jurisystem*

Un service de notation des avocats exploité sur un site ne présente pas un caractère trompeur et délivre une information loyale, claire et transparente à la condition de communiquer les critères de référencement.

Faits. – La société Jurisystem, spécialisée dans l'édition de supports juridiques, a créé, en 2012, le site avocat.net, devenu alexia.fr, afin de mettre en rapport des particuliers avec des avocats inscrits sur le site qui se présentait comme le « comparateur d'avocats n°1 en France » ; que, soutenant que la société Jurisystem, en exploitant son site, faisait un usage prohibé du titre d'avocat pour proposer des services juridiques, accomplissait des actes de démarchage interdits, se livrait à des pratiques trompeuses et contrevenait aux règles de la profession prohibant toute mention publicitaire comparative ainsi que la rémunération de l'apport d'affaires et le partage d'honoraires, le Conseil national des barreaux l'a assignée en interdiction de telles pratiques portant atteinte à l'intérêt collectif de la profession et en indemnisation.

Par un arrêt du 18 décembre 2015, la cour d'appel de Paris a interdit à la société Jurisystem de procéder et d'établir des comparateurs et notations d'avocat sur son site www.alexia.fr.

Dans son arrêt du 11 mai 2017, la première chambre civile de la Cour de cassation a partiellement cassé et annulé cet arrêt, au visa de l'article 15 du décret n° 2005-790 juillet 2005 et l'article L 121-1 du code de la consommation dans sa rédaction issue de la loi n°2008-776 du 4 août 2008, pour violation de la loi. La Haute juridiction considère que les tiers ne sont pas tenus par les règles déontologiques de la profession d'avocat et qu'il leur appartient seulement, dans leurs activités propres, de délivrer aux consommateurs une information loyale, claire et transparente.

La Cour de cassation a renvoyé l'affaire devant la cour d'appel de Versailles qui était appelée à statuer sur le caractère loyal, clair, transparent de la notation et du référencement d'avocats pratiqué sur ce site internet.

ARRÊT (Extrait)

« (…) Considérant que la société Jurisystem indique et justifie avoir supprimé de son site internet www.alexia.fr tout système de notation, ce que ne conteste pas ; que le conseil national des barreaux demande toutefois à la cour de renvoi de dire que ce système présentait un caractère trompeur et délivré une information qui n'était ni loyale, ni claire ni transparente, (…) ; qu'il faut donc comprendre que cette demande concerne la période antérieure à l'arrêt de la cour d'appel de Paris du 18 décembre 2015 ; qu'il demande également la communication permanente des critères de référencement et de comparaison des avocats et une mesure d'interdiction de la notation et de la comparaison des avocats sur le site www.alexia.fr (…) ; qu'il faut donc comprendre que ces demandes s'attachent à la période postérieure à l'arrêt de la cour d'appel de Paris du 18 décembre 2015 ; qu'il convient donc de distinguer les deux périodes ;

Mais considérant que s'il résulte de ces explications de la société Jurisystem qu'il existait bien des critères de référencement, il n'en résulte pas, qu'une information loyale, claire et transparente sur les conditions générales d'utilisation du service d'intermédiation et sur les modalités de référencement, de classement et de déréférencement des offres mises en ligne ait été délivrée aux consommateurs conformément à ce qu'exigeait l'article L 111-5-1 du code de la consommation ci-dessus rappelé ; qu'il convient donc de dire que jusqu'à l'arrêt de la cour d'appel de Paris du 18 décembre 2015, le service de notation des avocats exploité sur le site www.alexia.fr présentait un caractère trompeur en ce qu'il délivrait une information qui n'était ni loyale, ni claire ni transparente ; que cette pratique trompeuse porte atteinte à l'intérêt collectif de la profession d'avocat défendu par le conseil national des barreaux ; qu'il est donc fondé à réclamer une indemnité de un euro en réparation de son préjudice ;

Considérant que les critères de référencement ont été communiqués en cours de procédure ; que la société Jurisystem justifie qu'un lien hypertexte permet d'y accéder ; que le conseil national des barreaux ne prouve, ni même n'allègue, qu'elle ne délivre pas une information loyale, claire et transparente ; qu'il ne demande d'ailleurs pas à la cour de le constater ; que ses demandes visent en particulier à ce que la société Jurisystem communique de façon permanente les critères de référencement et de comparaison utilisés sur son site, à interdire la notation et la comparaison des avocats tant que l'intégralité des critères de référencement et de comparaison et leurs coefficients ne seront pas communiqués sur la page d'accueil de son site de façon permanente ainsi qu'à d'autres mesures in futurum ;

Considérant en effet qu'il s'agit de faits futurs qui ne sont pas dans le débat ; (…) qu'il n'est pas contesté que le système a été modifié depuis ; que les demandes d'interdiction à l'avenir présentent un caractère général qui ne permet pas de retenir l'existence d'une situation dommageable illicite justifiant qu'il en soit ordonné la cessation avant même la réalisation d'un préjudice ».

Références doctrinales :
- C.-S. Pinat, « Affaire Jurisystem : la décision lacunaire de la cour d'appel de renvoi », *Dalloz actualité,* 20 décembre 2018.

1- CJUE, 25 janvier 2018, n° C-498/16, *aff. Schrems*

L'article 15 du règlement (CE) no 44/2001 du Conseil, du 22 décembre 2000, concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, doit être interprété en ce sens qu'un utilisateur d'un compte Facebook privé ne perd pas la qualité de « consommateur », au sens de cet article, lorsqu'il publie des livres, donne des conférences, exploite des sites Internet, collecte des dons et se fait céder les droits de nombreux consommateurs afin de faire valoir ces droits en justice.

L'article 16, paragraphe 1 de ce même règlement doit être interprété en ce sens qu'il ne s'applique pas à l'action d'un consommateur visant à faire valoir, devant le tribunal du lieu où il est domicilié, non seulement ses propres droits, mais également des droits cédés par d'autres consommateurs domiciliés dans le même État membre, dans d'autres États membres ou dans des États tiers.

Faits - En l'espèce, M Schrems poursuit Facebook Ireland pour violation de ses obligations en matière de protection des données, non seulement en son nom propre mais également au nom d'autres utilisateurs lui ayant cédé les droits sur leurs comptes facebook. M Schrems se fonde sur la compétence internationale en tant que for du consommateur au visa de l'article 16, paragraphe 1, du règlement no 44/2001 pour attraire Facebook devant les juridictions autrichiennes. La question qui se posait à la CJUE était alors de savoir si M Schrems était bien un consommateur au sens du règlement CE n° 44/2001 article 15 et si l'article 16 de ce même règlement permettait à la juridiction du consommateur de connaître du litige non seulement pour la défense de ses droits propres de ce dernier, mais également sur les droits qui lui auraient été cédés.

ARRÊT (Extrait)

« […] la Cour a précisé que la notion de « consommateur », au sens des articles 15 et 16 du règlement no 44/2001, doit être interprétée de manière restrictive, en se référant à la position de cette personne dans un contrat déterminé, en rapport avec la nature et la finalité de celui-ci, et non pas à la situation subjective de cette même personne […].

La Cour en a déduit que seuls les contrats conclus en dehors et indépendamment de toute activité ou finalité d'ordre professionnel, dans l'unique but de satisfaire aux propres besoins de consommation privée d'un individu, relèvent du régime particulier prévu par ledit règlement en matière de protection du consommateur en tant que partie réputée faible […].

En ce qui concerne plus particulièrement une personne qui conclut un contrat pour un usage se rapportant en partie à son activité professionnelle et n'étant donc qu'en partie seulement étranger à celle-ci, la Cour a considéré qu'elle pourrait bénéficier desdites dispositions seulement dans l'hypothèse où le lien dudit contrat avec l'activité professionnelle de l'intéressé serait si ténu qu'il deviendrait marginal […].

La notion de consommateur […] est indépendante des connaissances et des informations dont la personne concernée dispose réellement […] ni l'expertise que cette personne peut acquérir dans le domaine duquel relèvent lesdits services ni son engagement aux fins de la représentation des droits et des intérêts des usagers de ces services ne lui ôtent la qualité de « consommateur » […].

Ensuite, la Cour a déjà relevé que le régime particulier institué aux articles 15 et suivants du règlement no 44/2001 étant inspiré par le souci de protéger le consommateur en tant que partie au

contrat réputée économiquement plus faible et juridiquement moins expérimentée que son cocontractant, le consommateur n'est protégé qu'en tant qu'il est personnellement demandeur ou défendeur dans une procédure. Dès lors, le demandeur qui n'est pas lui-même partie au contrat de consommation en cause ne saurait bénéficier du for du consommateur […]. Ces considérations doivent également valoir à l'égard d'un consommateur cessionnaire de droits d'autres consommateurs.

[…] le fait pour le cessionnaire consommateur de pouvoir, en tout état de cause, introduire, devant le tribunal du lieu de son domicile, une action au titre des droits qu'il tire personnellement d'un contrat conclu avec le défendeur, analogues à ceux qui lui ont été cédés, n'est pas de nature à faire également relever ces derniers de la compétence de ce tribunal ».

Références Doctrinales :
- D. Berlin**,** « Action collective et solitude du consommateur **»,** *JCP G* n° 6, 5 Février 2018, p.152.

2- TGI Paris 7 août 2018*, UFC Que Choisir c/ Twitter*

L'utilisateur d'un réseau social doit être considéré comme un consommateur, le contrat qui lie ce dernier à la plateforme doit ainsi respecter les dispositions du code de la consommation et ne peut contenir de clause abusive.

Faits - En l'espèce, l'association UFC QUE-CHOISIR demande l'application du droit de la consommation au réseau social TWITTER, selon ce dernier, le contrat d'utilisation est un contrat gratuit et exclut ainsi l'application des dispositions du droit de la consommation. L'association conteste la gratuité du service rendu aux utilisateurs de la plate-forme et demande à ce que certaines clauses des "Conditions Générales d'Utilisation" de TWITTER soient déclarées abusives et réputées non écrites dans tous les contrats proposés par TWITTER.

ARRÊT (Extrait)

« Il résulte de ce qui précède que, si la société TWITTER propose aux utilisateurs de la plate-forme des services dépourvus de contrepartie monétaire, elle commercialise à titre onéreux auprès d'entreprises partenaires, publicitaires ou marchands, des données, à caractère personnel ou non, déposées gratuitement par l'utilisateur à l'occasion de son inscription sur la plate-forme et lors de son utilisation.

Ainsi, la fourniture de données collectées gratuitement puis exploitées et valorisées par TWITTER doit s'analyser en un "avantage" au sens de l'article 1107 du code civil, qui constitue la contrepartie de celui que

TWITTER procure à l'utilisateur, de sorte que le contrat conclu avec TWITTER est un contrat à titre onéreux.

En conséquence, en collectant des données déposées gratuitement par l'utilisateur à l'occasion de son accès à la plate-forme et en les commercialisant à titre onéreux, la société TWITTER, agissant à des fins commerciales, tire profit de son activité, de sorte qu'il est un "professionnel" au sens de l'article liminaire du code de la consommation […].

Au surplus, les dispositions de l'article L. 121-1 du code de la consommation […] n'exigent pas que le contrat soit conclu à titre onéreux, seule la qualité des parties au contrat (professionnel/consommateur), déterminant l'application desdites dispositions […].

D’où il suit que le contrat d’utilisation de la plate-forme, exploitée par la société TWITTER en sa qualité de professionnel, est soumis aux dispositions du code de la consommation, notamment aux dispositions relatives aux clauses abusives, l’utilisateur qui participe au contenu restant un consommateur au regard des dispositions du code de la consommation ».

Références Doctrinales :

- G. Raymond, « Contrat d'adhésion à un réseau social : clauses abusives ou illicites » *JCP G,* n° 41, 8 oct. 2018, p. 1046.
- G. Loiseau, « Twittez, vous êtes consommateurs », *Communication Commerce électronique,* n° 10, oct. 2018, comm. 74.

TEXTES

1- Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel, *JORF* n° 0288 du 13 décembre 2018

Cette ordonnance a principalement pour objectif de mettre en conformité la loi n° 78-17 du 6 janvier 1978 Informatique et Libertés par rapport au RGPD ainsi que toute législation applicable en matière de données à caractère personnel. De ce fait, l'ordonnance va insérer dans la loi Informatique et liberté un certain nombre de références et de dispositions contenues dans le RGPD. A titre d'exemple, on pensera notamment aux trois critères d'application du champ territorial du RGPD (art. 3, RGPD), le droit à la limitation du traitement (art. 18, RGPD), ou encore le droit à la portabilité des données (art. 20, RGPD). Cette ordonnance modifie également les législations applicables en matière de données à caractère personnel prévues en dehors de la loi Informatique et Libertés.

2- Décret n° 2018-687 du 1er août 2018 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, *JORF* n° 0177 du 3 août 2018

Ce décret contient plusieurs mesures d'application de la loi n°2018-493 du 20 juin 2018. Parmi celles-ci, il convient de relever qu'il a défini les conditions dans lesquelles, soit la Commission nationale de l'informatique et des libertés soit l'organisme national d'accréditation mentionné au b du 1 de l'article 43 du règlement (UE) 2016/679, agrée les organismes certificateurs aux fins de reconnaître qu'ils se conforment au règlement (UE) 2016/679 et à la loi du 6 janvier 1978.

Y sont notamment être précisées les conditions dans lesquelles les membres et agents de la commission amenés à réaliser des opérations en ligne nécessaires à leur mission sous une identité d'emprunt procèdent à leurs constatations. Il définit la procédure d'urgence contradictoire appliquée par la formation restreinte saisie par le président de la Commission nationale de l'informatique et des libertés. Il pose également les conditions d'application de l'article 49-3 de loi du 6 janvier 1978, relatif au traitement transfrontalier au sein de l'Union européenne.

3- Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, *JORF* n° 0141 du 21 juin 2018

La loi relative à la protection des données personnelles a été promulguée le 20 juin 2018. Elle adapte la loi "Informatique et libertés" du 6 janvier 1978 au "paquet européen de protection des données". Ce paquet se compose du règlement général sur la protection des données (RGPD), d'un règlement du 27 avril 2016 directement applicable dans tous les pays européens au 25 mai 2018 ainsi que d'une directive du même jour sur les fichiers en matière pénale, dite directive "police".

Se faisant, la loi fondatrice du 6 janvier 1978 se trouve modifiée sur plusieurs points pour la mettre en conformité avec le RGPD (missions et pouvoirs de la CNIL, élargissement des données sensibles) ou tirer parti des marges de manœuvre qu'il permet (majorité numérique, etc.).

4- Règlement (UE) 2016/79 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *JOUE* L 119/1 (RGDP)

Le règlement RGPD a pour but d'établir des règles relatives à la protection des personne physiques à l'égard du traitement des données à caractère personnel, et de poser les règles relatives à la libre circulation de ces données. Ce règlement a vocation à s'appliquer lors d'un traitement de données à caractère personnel, qu'il soit automatisé ou non lorsque les données ont vocation à figurer dans un fichier. Sont visés les traitements des données à caractère personnel par les institutions, organes et organismes de l'Union.

JURISPRUDENCE

I- Formalités

1- Cour d'Appel de Paris, chambre 8, 1er mars 2019, *M. X. c/ Oxeva*

La responsabilité civile d'un hébergeur ne peut être engagée qu'après notification du contenu illicite, et ce antérieurement à l'action en justice.

Faits - La société Oxeva, dont l'activité principale est l'hébergement ainsi que la création de sites internet avait associé, par une multitude de sites, le nom et l'activité de M. X., avocat, à des numéros de téléphone surtaxés n'étant pas les siens. Après qu'aucune suite n'ait été donnée à une lettre de mise en demeure du 3 mars 2017, et arguant d'un détournement de clientèle, celui-ci fait assigner la société Oxeva devant le tribunal de grande instance de Paris le 23 mars 2017 afin d'engager la responsabilité civile de la société et de faire retirer l'ensemble de ses informations personnelles sur quelque site ou emplacement que ce soit.

Par une ordonnance du 18 mai 2018, le tribunal déboute M. X. de toutes ses demandes. Le premier juge a rejeté les demandes en retenant principalement que le demandeur n'avait pas établi, alors que la société Oxeva est hébergeur de contenu, la notification préalable des contenus illicites au sens de la loi du 21 juin 2004, de sorte que la responsabilité civile de la Société ne peut être engagée.

La cour d'Appel va confirmer le jugement de première instance. Se basant sur les articles 6.1.2 de la loi du 21 juin 2004, et 6.1.5 de la même loi, les juges vont estimer que M. X. ne justifiait pas de la notification préalable en cas de contenus illicites. Ce faisant, la responsabilité civile de la société ne pouvait être engagée.

ARRÊT (Extrait)

« (…) Il est constant que la loi n°2004-575 du 21 juin 2004 pour la confiance en l'économie numérique instaure un régime de responsabilité civile et pénale de la personne physique ou morale poursuivie différents selon la qualité d'hébergeur ou d'éditeur des sites.
En l'espèce, il a été parfaitement expliqué par le premier juge que la société Oxeva est intervenue en qualité d'hébergeur des deux sites litigieux.

(…) Or, l'article 61.2 de la loi susvisée dispose que : « Les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent pas voir leur responsabilité civile

engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible ».
En outre, l'article 6.1.5 exige pour les hébergeurs, une notification des contenus illicites contenant les éléments prévus par ladite loi, notamment la copie de la correspondance adressée à l'auteur ou à l'éditeur des informations ou activités litigieuses demandant leur interruption, leur retrait ou leur modification.

Ainsi, il résulte du dispositif mis en place que la responsabilité de l'hébergeur ne peut être engagée que lorsque plusieurs conditions cumulatives sont réunies. Le contenu litigieux doit être manifestement illicite, la personne qui souhaite faire retirer le contenu s'adresse à l'auteur ou à l'éditeur du site et sollicite en motivant sa demande de retrait. En cas d'absence de réponse positive, la personne peut s'adresser à l'hébergeur en lui notifiant les démarches accomplies, la copie du courrier adressé à l'éditeur ou à l'auteur en lui fournissant les informations prévues à l'article 6-1-5 de la loi LCEN.

(…) Si M. X. a justifié avoir adressé à la société Oxeva un courrier recommandé avec accusé de réception le 3 mars 2017, antérieur à l'assignation délivrée à l'éditeur, le contenu de cette lettre est finalement contesté par la société Oxeva qui a pris soin, dès sa réception et par l'intermédiaire de son conseil, suivant un courrier en réponse du 23 mars 2017 d'indiquer que l'enveloppe ne contenait qu'une page d'un site « Village Justice » et l'invitait à s'expliquer sur cette transmission.
(…) Par ailleurs, il n'est justifié, ni prétendu, d'aucune notification du contenu illicite relative au site.

Ainsi c'est à bon droit que le premier juge a retenu que la société Oxeva ayant la qualité d'hébergeur de contenus, M. X. ne justifiait pas de la notification préalable en cas de contenus illicites prévue par la loi du 21 juin 2001 et que sa responsabilité civile ne pouvait être engagée. »

2- Cour de Justice de l'Union Européenne, Grande chambre, 5 juin 2018, C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c/ Wirtschaftsakademie Schleswig-Holstein GmbH*

L'administrateur d'une page fan sera qualifié de responsable de traitement au sein de l'Union, conjointement avec Facebook, et pourra ainsi voir sa responsabilité engagée en cas de manquement.

Faits – Dans le cadre d'un litige opposant l'Unabhängiges Landeszentrum fur Datenschutz Schleswig-Holstein (autorité régionale indépendante de protection des données du Schleswig-Holstein, Allemagne) (ci-après l'" ULD ") à Wirtschaftsakademie Schleswig-Holstein GmbH, société de droit privé spécialisée dans le domaine de l'éducation (ci-après "la Société"), une question préjudicielle portant sur l'interprétation de la directive 95/46/CE du Parlement Européen, relative à la protection des personne physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données est posée à la Cour.

L'ULD avait en effet émis une injonction à la Société, le 3 novembre 2011, de désactiver sa page fan hébergée sur Facebook. Soucieuse du traitement des données à caractère personnel, l'ULD avait constaté que ni la Société, ni Facebook n'informait les visiteurs de la page fan que Facebook collectait, à l'aide de cookies, des informations à caractère personnel et qu'il traitait ensuite ces informations. Selon la Société, celle-ci n'était pas responsable du traitement ou des cookies installés par Facebook et avait donc introduit une réclamation. Par décision du 16 décembre 2011, l'ULD

rejette la réclamation en considérant que la responsabilité de la Société, en tant que fournisseur de service, était établie.

La Société introduit donc un recours contre cette décision devant le tribunal administratif allemand, en faisant valoir que le traitement des données à caractère personnel effectué par Facebook ne pouvait lui être imputé et qu'elle n'avait pas non plus chargé Facebook de procéder au traitement de données qu'elle contrôlerait ou qu'elle pourrait influencer. Selon elle, l'ULD aurait dû agir contre Facebook directement. Le tribunal administratif, le 9 octobre 2013, annule la décision. L'appel formé par l'ULD est également rejeté par le tribunal administratif supérieur allemand. Aussi, l'ULD introduit alors un recours en révision devant la cour administrative fédérale Allemande qui va solliciter la Cour de Justice de l'Union Européenne.

Se pose dès lors à la Cour la question de savoir si la directive 95/46 doit être interprétée en ce sens qu'elle permette de retenir la responsabilité d'un organisme, en sa qualité d'administrateur d'une page fan hébergée sur un réseau social, en cas d'atteinte aux règles relatives à la protection des données à caractère personnel, en raison du choix d'avoir recours à ce réseau social pour diffuser son offre d'informations.

Du fait de son action de paramétrage, la Cour retient que la Société participait activement et pouvait donc être qualifié de responsable du traitement. Dès lors, sa responsabilité pouvait être engagée, conjointement avec celle de l'exploitant du réseau social.

ARRÊT (Extrait)

« 35. Or, si le simple fait d'utiliser un réseau social tel que Facebook ne rend pas un utilisateur de Facebook coresponsable d'un traitement de données à caractère personnel effectué par ce réseau, il convient, en revanche, de relever que l'administrateur d'une page fan hébergée sur Facebook, par la création d'une telle page, offre à Facebook la possibilité de placer des cookies sur l'ordinateur ou sur tout autre appareil de la personne ayant visité sa page fan, que cette personne dispose ou non d'un compte Facebook. (…)

39. Dans ces circonstances, il y a lieu de considérer que l'administrateur d'une page fan hébergée sur Facebook, tel que Wirtschaftsakademie, participe, par son action de paramétrage, en fonction, notamment, de son audience cible ainsi que d'objectifs de gestion ou de promotion de ses activités, à la détermination des finalités et des moyens du traitement des données personnelles des visiteurs de sa page fan. De ce fait, cet administrateur doit être, en l'occurrence, qualifié de responsable au sein de l'Union, conjointement avec Facebook Ireland, de ce traitement, au sens de l'article 2, sous d), de la directive 95/46.

40. En effet, le fait pour un administrateur d'une page fan d'utiliser la plateforme mise en place par Facebook, afin de bénéficier des services y afférents, ne saurait l'exonérer du respect de ses obligations en matière de protection des données à caractère personnel. (…)

42. Dans ces conditions, la reconnaissance d'une responsabilité conjointe de l'exploitant du réseau social et de l'administrateur d'une page fan hébergée sur ce réseau en relation avec le traitement des données personnelles des visiteurs de cette page fan contribue à assurer une protection plus complète des droits dont disposent les personnes qui visitent une page fan, conformément aux exigences de la directive 95/46.

(…)

44. Au regard des considérations qui précèdent, il y a lieu de répondre aux première et deuxième questions que l'article 2, sous d), de la directive 95/46 doit être interprété en ce sens que la notion de "responsable du traitement", au sens de cette disposition, englobe l'administrateur d'une page fan hébergée sur un réseau social ».

II- Consentement

Conseil d'État 10e et 9e chambres réunies, 6 juin 2018, *Editions Croque Futur c/ Cnil,* n° 412589

Le Conseil d'Etat a détaillé les obligations pesant sur les responsables du traitement de données consistant en l'utilisation de « cookies », qui constitue un traitement de données.

Faits - Le 27 novembre 2014, la Commission National de l'Informatique et des Libertés (CNIL) diligente une mission de contrôle de la société Editions Croque futur et notamment de son site internet www.challenges.fr. Plusieurs manquements à la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés sont constatés.

Après mise en demeure infructueuse auprès des Editions Croque Futur, une formation restreinte de la CNIL leur inflige futur une sanction pécuniaire de 25 000 euros.

Les Editions Croque Futur forment un recours devant le Conseil d'Etat afin de faire annuler la sanction.

ARRÊT (Extrait)

« (…) Elles imposent, d'une part, une information des utilisateurs de services de communications électroniques, en particulier des utilisateurs d'internet, sur la finalité de ces " cookies " et les moyens dont ils disposent pour s'y opposer. Elles imposent, d'autre part, le recueil de leur consentement avant tout dépôt de " cookies " sur le terminal grâce auquel ils accèdent à ces services. Ne sont pas concernés par ces obligations les " cookies " qui sont essentiels au fonctionnement technique du site ni ceux qui correspondent à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur. En revanche, contrairement à ce que soutient la société, le fait que certains " cookies " ayant une finalité publicitaire soient nécessaires à la viabilité économique d'un site ne saurait conduire à les regarder comme " strictement nécessaires à la fourniture " du service de communication en ligne.

(…)

8. En premier lieu, alors que la société requérante soutient qu'elle s'est mise en conformité avec ces exigences dès le mois de juin 2016, en proposant aux personnes concernées le paramétrage de leur navigateur pour s'opposer au dépôt de " cookies ", il résulte de l'instruction que les éléments portés à la connaissance des utilisateurs du site" www.challenges.fr " ne leur permettaient ni de différencier clairement les catégories de " cookies " susceptibles d'être déposés sur leur terminal, ni de s'opposer seulement à ceux dont le dépôt est soumis à leur consentement préalable, ni de connaître les conséquences, en termes de navigation sur le site, attachées à leur éventuelle opposition. Dans ces conditions, c'est à bon droit que la formation restreinte de la CNIL a considéré que le paramétrage du navigateur proposé aux utilisateurs ne constituait pas un mode valable d'opposition au dépôt de " cookies " et en a déduit qu'il n'avait pas été remédié au manquement à l'obligation d'information et de mise en œuvre d'un mécanisme d'opposition en cas de dépôt de témoins de connexion.

(…)

11. L'utilisation de " cookies " répondant aux caractéristiques définies au II de l'article 32 de la loi du 6 janvier 1978 constitue un traitement de données qui doit respecter les prescriptions de l'article 6 précité. Lorsque des " cookies " sont déposés par l'éditeur du site, il doit être considéré comme responsable de traitement au sens de la loi. Il en va de même lorsque l'éditeur sous-traite à des tiers la gestion de " cookies " mis en place pour son compte. Les autres tiers qui déposent des " cookies " à l'occasion de la visite du site d'un éditeur doivent être considérés comme responsables de traitement. Toutefois, les éditeurs de site qui autorisent le dépôt et l'utilisation de tels " cookies " par des tiers à l'occasion de la visite de leur site doivent également être considérés comme responsables de traitement, alors même qu'ils ne sont pas soumis à l'ensemble des obligations qui s'imposent au tiers qui a émis le " cookie ", notamment lorsque ce dernier conserve seul la maitrise du respect de sa finalité ou de sa durée de conservation. Au titre des obligations qui pèsent sur l'éditeur de site dans une telle hypothèse, figurent celle de s'assurer auprès de ses partenaires qu'ils n'émettent pas, par l'intermédiaire de son site, des " cookies " qui ne respectent pas la règlementation applicable en France et celle d'effectuer toute démarche utile auprès d'eux pour mettre fin à des manquements.

(…)

12. Il résulte de l'instruction que la société n'a pas donné suite à la mise en demeure de définir et de respecter une durée de conservation des données qui ne soit pas supérieure à treize mois pour les " cookies " déposés à l'occasion de la visite du site qu'elle édite. En ce qui concerne les " cookies " déposés par des tiers, il résulte de l'instruction que ses allégations selon lesquelles elle aurait effectué des démarches auprès de ses partenaires afin qu'ils respectent une durée de conservation ne sont étayées d'aucun élément. Il s'ensuit que c'est à bon droit et sans méconnaître le principe de la responsabilité personnelle que la formation restreinte de la CNIL a estimé qu'il n'avait pas été remédié au manquement à l'obligation de définir et respecter une durée de conservation des données proportionnée à la finalité du traitement ».

Références Doctrinales :
-J. Larrieu, C. Le Stanc, P. Tréfigny « Droit du numérique », *Recueil Dalloz 2018*, p.2270
- E. Maupin, « L'utilisation de cookies constitue un traitement de données », *AJDA 2018*, p.1194.

DÉLIBÉRATIONS CNIL

I. Consentement libre, éclairé et spécifique

1- Délibération 2018-042 du 30 octobre 2018 mettant en demeure la société *Vectaury* (clôturée)

Mise en demeure pour absence de consentement au traitement de données de géolocalisation à des fins de ciblage publicitaire.

Faits - La société de ciblage publicitaire collectait les données de géolocalisation d'utilisateurs de smartphone sans leur consentement, et ce même lorsque l'application n'était pas utilisée. Elle a pour cela recours à des outils techniques dénommés « SDK ». Ces outils sont intégrés dans le code d'applications mobiles de leurs partenaires. De plus, l'utilisateur ne pouvait désactiver cette collecte des données au stade du téléchargement ou choisir de ne pas télécharger le SDK. Le Règlement européen sur la protection des données et la loi Informatique et libertés exigent un consentement libre et éclairé. La CNIL relevant que le consentement n'était pas valablement recueilli met en demeure la société à se mettre en conformité avec ces textes et de supprimer les données indûment collectées.

DÉLIBÉRATION (Extrait)

« (…) À cet égard, la notion de consentement, reprise dans le règlement général sur la protection des données, n'est pas moins exigeante dès lors qu'il est prévu que celui-ci doit être donné par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant.

Or, il ressort des contrôles et de l'analyse des pièces transmises à la Commission que le mécanisme proposé aux utilisateurs ayant téléchargé les applications des partenaires de la société ne permet pas aux utilisateurs de consentir valablement aux traitements opérés par cette dernière.

(…) En premier lieu, le consentement doit être informé. […]

En l'espèce, l'information relative à l'identité des responsables des traitements n'est pas directement accessible aux personnes. Elle nécessite que l'utilisateur, à l'ouverture de l'application, fasse le choix d'affiner ses préférences, et fasse défiler son écran jusqu'à atteindre un lien intitulé Voir tous les partenaires. Un clic sur ce lien le renverra vers une page listant tous les partenaires de l'application, dont VECTAURY.

Cette présentation implique qu'à l'affichage de la première page, où figurent les boutons cliquables J'accepte, Je refuse et J'affine mes préférences, l'utilisateur n'est pas informé des destinataires de ses données, et que l'éventuel consentement qu'il donnerait en cliquant sur le bouton J'accepte ne serait pas un consentement informé.

Par conséquent, et même dans l'hypothèse où la nouvelle version du CMP serait déployée sur l'intégralité des applications au sein desquelles la société VECTAURY a installé son SDK, les personnes ne sont pas dûment informées de la collecte de leurs données de géolocalisation par la société VECTAURY, via l'installation d'un SDK, à des fins de publicité ciblée. (…)

En deuxième lieu, le consentement doit être spécifique. […]

Si une facilité d'utilisation peut être proposée par un bouton d'acceptation ou de refus global, cette fonctionnalité ne peut pas lui être présentée avant que les différentes finalités du traitement ne lui soient exposées, faute de quoi l'utilisateur donnerait un consentement global à plusieurs traitements qu'il ne connaît pas et pour lesquels un consentement spécifique n'a pas été sollicité. Par sa présentation même, la gestion globale du consentement (acceptation ou refus) doit indiquer l'existence de plusieurs traitements ou de plusieurs finalités.

Une acceptation globale, sans même que l'utilisateur ne soit clairement informé de l'existence de plusieurs traitements ou de plusieurs finalités, ne saurait répondre au critère de spécificité du consentement exigé par le G29. (…)

(…) En dernier lieu, le consentement doit être exprimé par une action positive de l'utilisateur. […]

Dans cette nouvelle interface, l'utilisateur qui décide d'affiner ses préférences se voit informer des cinq finalités présentées par l'éditeur de l'application (conservation et accès aux informations, personnalisation, sélection, diffusion et signalement de publicités, sélection, diffusion et signalement de contenu et évaluation).

L'ensemble de ces finalités sont pré-acceptées par défaut.

Il résulte de tout ce qui précède que le consentement des personnes n'est pas valablement recueilli, et que les données jusqu'ici détenues et traitées par la société VECTAURY le sont sans base légale. (…) »

2- Délibération 2018-043 du 8 octobre 2018 mettant en demeure la société *Singlespot*

Mise en demeure pour absence de consentement au traitement de données de géolocalisation à des fins de ciblage publicitaire.

Faits - La société de ciblage publicitaire collectait les données de géolocalisation des utilisateurs de l'application via un SDK. L'utilisateur ne pouvait désactiver la collecte des données au stade du téléchargement, l'utilisation de l'application avait donc pour conséquence la transmission automatique des informations à la société VECTAURY. L'application organise aussi un système d'offre d'enchère d'espace publicitaire en temps réel, il y a là aussi un traitement des données récoltées activé par défaut. A ce stade, l'utilisateur n'était pas informé de la finalité du ciblage publicitaire ou de l'identité du responsable de ce traitement. Ces informations étaient fournies après traitement des données dans les conditions générales d'utilisation, alors que le consentement suppose une information préalable. La CNIL met en demeure la société à récolter préalablement le consentement effectif des utilisateurs concerner et de supprimer les données indûment récoltées.

DÉLIBÉRATION (Extrait)

« **En premier lieu**, le consentement des personnes doit être informé.

Le G29 indique, dans ses lignes directrices du 10 avril 2018 sur le consentement au sens du Règlement 2016/679, que le responsable du traitement doit s'assurer que le consentement est fourni sur la base d'informations qui permettent aux personnes concernées d'identifier facilement qui est le responsable des données et de comprendre ce à quoi elles consentent. [Il] doit clairement décrire la finalité du traitement des données pour lequel le consentement est sollicité. […]

En l'espèce, la délégation a constaté qu'au moment de l'installation des applications contrôlées, les personnes ne sont pas informées de la collecte de leurs données de géolocalisation via le SDK à des fins de profilage des utilisateurs et de ciblage publicitaire.

En deuxième lieu, le consentement doit être spécifique.

[…] Le RGPD établit clairement que le consentement nécessite une déclaration de la part de la personne concernée ou un acte positif clair, ce qui signifie qu'il doit toujours être donné par une déclaration ou un geste actif. […] Le silence ou l'inactivité de la personne concernée, ainsi que le simple fait qu'elle continue à utiliser un service, ne peuvent être considérés comme une indication active de choix.

En l'espèce, la délégation a constaté à l'occasion du contrôle sur place que les personnes sont amenées à valider l'autorisation système de collecter leurs données de géolocalisation uniquement pour l'utilisation globale de l'application mobile téléchargée. […]

En dernier lieu, le consentement doit être univoque.

Les lignes directrices WP 259 sur le consentement adoptées le 28 novembre 2017 retiennent que le consentement ne constitue une base juridique appropriée que si la personne concernée dispose d'un contrôle et d'un choix réel concernant l'acceptation ou le refus des conditions proposées.

La fenêtre contextuelle précitée offre à l'utilisateur deux onglets cliquables : j'accepte ou plus tard. Aucune de ces options ne lui propose clairement de refuser la collecte et le traitement de ses données à caractère personnel.

Dès lors, le consentement donné n'est pas univoque. »

3- Délibération n° 2018-023 du 25 juin 2018 mettant en demeure la société *Fidzup*

Mise en demeure pour absence de consentement au traitement de données de géolocalisation à des fins de ciblage publicitaire.

Faits - La société de ciblage publicitaire collectait des données de géolocalisation des utilisateurs de l'application, si ce dernier pouvait désactiver la collecte des données au stade du téléchargement, cette option ne concernait pas la collecte des données via le SDK présent dans les applications partenaires. De plus, l'utilisateur n'était pas informé à ce stade de la finalité du ciblage publicitaire ou de l'identité du responsable de ce traitement. Ces informations étaient fournies après la collecte et le traitement des données dans les conditions générales d'utilisation et les affiches en magasin, alors que le consentement suppose une information préalable. De plus, il n'était pas possible de télécharger l'application sans le SDK. La CNIL met en demeure la société à se conformer à la loi informatique et liberté et au RGPD dans un délai de 3 mois.

DÉLIBÉRATION (Extrait)

« **En premier lieu**, le consentement doit être informé.

[…] la notion de consentement, reprise dans le règlement général sur la protection des données, n'est pas moins exigeante dès lors qu'il est prévu que celui-ci doit être donné *par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant,*

Or, il ressort de l'analyse des pièces transmises à la Commission et du contrôle du 24 avril 2018 qu'aucun mécanisme n'est proposé aux utilisateurs ayant téléchargé les applications des partenaires de la société pour consentir préalablement aux traitements opérés par cette dernière […]

En deuxième lieu, les utilisateurs des applications ne fournissent pas un consentement libre au traitement réalisé par la société.

Dans son avis n°15/2011 du 13 juillet 2011, le G29 considère que *Le consentement ne peut être valable que si la personne concernée est véritablement en mesure d'exercer un choix et s'il n'y a pas de risque de tromperie […] Si les conséquences du consentement sapent la liberté de choix des personnes, le consentement n'est pas libre.*

Or, en l'espèce, la délégation a été informée, lors du contrôle du 14 septembre 2017, que les applications des éditeurs partenaires qui utilisent le SDK n'existent pas dans une version sans celui-ci et que par conséquent, les personnes ne peuvent télécharger les applications mobiles sans télécharger le SDK. Ce traceur est donc indissociable des applications partenaires.

En conséquence, les utilisateurs des applications mobiles ne sont pas libres de consentir au traitement des données réalisé par la société FIDZUP [...]

En troisième lieu, il apparait que les personnes ne fournissent pas un consentement spécifique à la collecte de leurs données personnelles à des fins publicitaires et le cas échéant, à des fins de ciblage réalisé à partir de leur localisation.

Dans un avis 15/2011 du 13 juillet 2011, le G29 a rappelé que : *Pour être valable, le consentement doit être spécifique. En d'autres termes, un consentement général, sans préciser la finalité exacte du traitement, n'est pas acceptable.*

S'agissant du pop-up *proposé et recommandé aux éditeurs* par la société FIDZUP, afin d'informer les utilisateurs du traitement de leurs données *à des fins de marketing ciblé*, la délégation a constaté, lors du contrôle du 24 avril 2018, qu'aucun mécanisme permettant de recueillir le consentement spécifique des personnes à la collecte de leurs données à des fins de ciblage publicitaire ne s'affiche lors du téléchargement et de l'utilisation des applications mobiles contrôlées.

En outre, la délégation a constaté que les personnes sont amenées à valider l'autorisation de la collecte de leurs données, y compris de localisation, uniquement pour l'utilisation de l'application mobile téléchargée. Elles ne fournissent donc pas de consentement spécifique au traitement de leurs données à des fins de ciblage publicitaire, le cas échéant géolocalisé. »

II- Sécurité

1- Délibération n° SAN-2019-001 du 21 janvier 2019, *Google LLC*

La CNIL a prononcé le 21 janvier 2019 une sanction de 50 millions d'euros à l'encontre de Google LLC en application du RGPD pour manque de transparence, information insatisfaisante et absence de consentement préalable.

Faits - Les associations None Of Your Business (NOYB) et La Quadrature du Net (LQDN) déposent deux plaintes contre Google LLC en mai 2018.

L'association NOYB reproche à Google le fait que les utilisateurs de terminaux mobiles Android sont tenus d'accepter la politique de confidentialité et les conditions générales d'utilisation des services de Google et qu'à défaut d'une telle acceptation, ils ne pourraient utiliser leur terminal.

L'association LQDN estime quant à elle, qu'indépendamment du terminal utilisé, Google ne dispose pas de bases juridiques valables pour mettre en œuvre les traitements de données à caractère personnel à des fins d'analyse comportementale et de ciblage publicitaire.

Un contrôle en ligne est effectué en septembre 2018 afin de vérifier la conformité de tout traitement relatif à l'utilisation du système Android à la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et au RGPD.

A l'issue de l'instruction, un rapport détaillant les manquements relatifs aux articles 6, 12 et 13 du RGPD propose le prononcé d'une sanction pécuniaire de 50 millions d'euros, rendue publique.

DÉLIBÉRATION (Extrait)

« (…) 4. Sur le manquement aux obligations de transparence et d'information (…)

(…) En l'espèce, la formation restreinte constate que l'architecture générale de l'information choisie par la société ne permet pas de respecter les obligations du Règlement. En effet, les informations qui doivent être communiquées aux personnes en application de l'article 13 sont excessivement éparpillées dans plusieurs documents : Règles de confidentialité et conditions d'utilisation, affiché au cours de la création du compte, puis Conditions d'utilisation et Règles de confidentialité qui sont accessibles dans un deuxième temps au moyen de liens cliquables figurant sur le premier document. Ces différents documents comportent des boutons et liens qu'il est

nécessaire d'activer pour prendre connaissance d'informations complémentaires. Un tel choix ergonomique entraine une fragmentation des informations obligeant ainsi l'utilisateur à multiplier les clics nécessaires pour accéder aux différents documents. […]

La formation restreinte relève que, compte tenu de cette architecture, certaines informations sont difficilement trouvables. (…)

(…) La formation restreinte relève encore que si l'utilisateur souhaite disposer d'information sur les durées de conservation de ses données personnelles, il doit tout d'abord consulter les Règles de confidentialité qui se trouvent dans le document principal, puis se rendre dans la rubrique intitulée Exporter et supprimer vos informations et enfin cliquer sur le lien hypertexte cliquer ici contenu dans un paragraphe général sur les durées de conservations. Ce n'est donc qu'au bout de quatre clics que l'utilisateur accède à cette information. La formation restreinte constate au demeurant que le titre choisi par la société pour Exporter et supprimer vos informations ne permet pas facilement à l'utilisateur de comprendre qu'il s'agit d'une rubrique permettant d'accéder aux informations relatives aux durées de conservation. Dès lors, la formation restreinte estime dans ce cas de figure que la multiplication des actions nécessaires, combinée à un choix de titres non explicites ne satisfait pas aux exigences de transparence et d'accessibilité de l'information.

Il résulte de l'ensemble de ces éléments un défaut global d'accessibilité des informations délivrées par la société dans le cadre des traitements en cause. (…)

(…) la formation restreinte estime que l'utilisateur n'est pas en mesure, en particulier en prenant connaissance du premier niveau d'information qui lui est présenté dans les Règles de confidentialité et conditions d'utilisation , de mesurer la portée des principaux traitements sur sa vie privée. Si elle prend acte de ce qu'une information exhaustive, dès le premier niveau, serait contreproductive et ne respecterait pas l'exigence de transparence, elle estime que celui-ci devrait contenir des termes de nature à objectiver le nombre et la portée des traitements mis en œuvre. Elle considère en outre qu'il serait possible, par d'autres types de modalités de présentation adaptées à des services de combinaison de données, de fournir dès le stade des Règles de confidentialité une vision d'ensemble des caractéristiques de cette combinaison en fonction des finalités poursuivies. (…)

(…) La formation restreinte souligne que si devant elle, la société a indiqué que la seule base juridique sur laquelle repose le traitement relatif à la publicité personnalisée est le consentement, il ressort de l'instruction que cette clarification n'est pas portée à la connaissance des utilisateurs. Les formulations rappelées ci-dessus ne permettent pas à ces derniers de mesurer clairement la distinction entre la publicité proprement personnalisée, à partir de la combinaison de multiples données relatives à l'utilisateur, qui repose d'après les dires de la société sur le consentement, d'autres formes de ciblage utilisant par exemple le contexte de navigation, fondées sur l'intérêt légitime. (…)

(…) Au regard de l'ensemble de ces éléments, la formation restreinte considère qu'un manquement aux obligations de transparence et d'information telles que prévues par les articles 12 et 13 du Règlement est caractérisé. (…)

(…)5. Sur le manquement à l'obligation de disposer d'une base légale pour les traitements mis en œuvre (…)

(…) La formation restreinte relève que les modalités d'expression du consentement ont été précisées et définies par l'article 4 (11) du Règlement, qui indique que l'on entend par consentement : toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la

personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Ces mêmes modalités d'expression du consentement s'appliquent de la même manière, que le consentement soit recueilli, au titre de l'article 6 du RGPD, pour la mise en œuvre d'un traitement pour une finalité spécifique, ou qu'il soit recueilli, en application de l'article 9 du RGPD, pour lever l'interdiction de principe posée au traitement de données à caractère personnel dites sensibles.
Par conséquent, pour pouvoir être considéré comme valable, le consentement recueilli doit être une manifestation volonté spécifique, éclairée et univoque ce qui, comme la formation restreinte l'a relevé précédemment, n'est pas le cas en l'espèce.

Au vu de l'ensemble de ces éléments, la formation restreinte considère que le consentement sur lequel se fonde la société pour les traitements de personnalisation de la publicité n'est pas valablement recueilli. (…)

(…) La formation restreinte de la CNIL, après en avoir délibéré, décide :

de prononcer à l'encontre de la société Google LLC, une sanction pécuniaire d'un montant de 50 (cinquante) millions d'euros ;

d'adresser cette décision à la société Google France Sarl en vue de l'exécution de cette décision ;

de rendre publique sa délibération, sur le site de la CNIL et sur le site de Légifrance, qui sera anonymisée à l'expiration d'un délai de deux ans à compter de sa publication. (…) »

Références Doctrinales :
- J. Deroulez, « Données à caractère personnel - Google condamné à une sanction pécuniaire de 50 millions d'euros par la CNIL : la révolution du consentement ? », *JCP* G, n° 4, 28 Janvier 2019, 67.
- J. Deroulez, « Données personnelles - Délibération de la CNIL du 21 janvier 2019 à l'encontre de Google LLC : portée et appréciation d'une décision symbolique », *JCP* E n° 6, 7 Février 2019, 1059.

2- Délibération de la formation restreinte n° SAN-2018-012 du 26 décembre 2018 prononçant une sanction pécuniaire à l'encontre de la société *Bouygues Telecom* (250.000€)

Se limitant à une seule mesure de sécurité afin de protéger les données personnelles de ses clients, la société Bouygues aurait dû lui accorder une attention renforcée afin d'éviter toute brèche informatique.

Faits - A la suite d'une détection faille informatique de leur site, Bouygues Telecom notifie à la CNIL la violation de données à caractère personnel le 6 mars 2018. En modifiant la fin d'une URL, il était possible d'accéder au contrat d'un autre client de la société et d'avoir accès ainsi à un certain nombre d'informations personnelles. Le 9 mars 2018, une délégation de la CNIL procède à une mission de contrôle dans les locaux de la société BOUYGUES TELECOM. Elle constate la résolution du problème, mais en interrogeant sur la date à laquelle le défaut de sécurité était apparu, la société a expliqué que la vulnérabilité trouvait son origine dans la fusion en 2015 des marques Bouygues Telecom et B&You et des systèmes informatiques correspondants.

À l'occasion de tests effectués à la suite de la fusion de ces bases de données, le code informatique rendant nécessaire l'authentification au site web www.bouyguestelecom.fr avait été désactivé. En raison d'une erreur humaine commise par une personne agissant pour le compte de la société, ce code n'a pas été réactivé à l'issue des tests réalisés.

Selon la CNIL, si la société a bien respecté les règles de l'art en mettant en place au moment de la fusion un mécanisme rendant l'authentification de l'utilisateur nécessaire avant de lui permettre d'accéder aux données sur le site, la formation restreinte retient que Bouygues a fait le choix de ne pas instaurer de mesure complémentaire de protection. Ce faisant, pesait alors sur la société une obligation particulièrement renforcée quant à la vigilance qu'il convenait de porter à cette unique mesure de sécurité.

Quand bien même la société avait réalisé des tests de sécurité, la formation restreinte constate que ces tests n'étaient pas adaptés aux spécificités de la base héritée et qu'ils ne pouvaient amener à la découverte de la vulnérabilité. Ces tests étaient donc inefficaces en l'espèce.

Elle en conclut que la société n'a pas apporté l'attention nécessaire à la base pour assurer la sécurité des données personnelles traitées et inflige donc à la société une sanction pécuniaire de 250 000 euros.

DÉLIBÉRATION (Extrait)

« (…) En premier lieu, sur la mesure de protection mise en place, la société considère qu'elle a respecté les règles de l'art en mettant en place, au moment de la fusion de ses systèmes d'information, un mécanisme rendant nécessaire l'authentification de l'utilisateur avant de lui permettre d'accéder aux données sur le site web www.bouyguestelecom.fr. Elle considère qu'une seconde mesure de protection, telle que le fait de rendre les adresses URL imprévisibles ou difficilement lisibles, n'est une pratique imposée ni par les textes, ni par l'état de l'art.

Sur ce point, la formation restreinte constate que l'article 34 précité n'est pas prescriptif quant aux mesures devant être déployées par les responsables de traitement pour garantir la sécurité d'un traitement tant que l'obligation est, in fine, respectée.

La formation restreinte considère ainsi que bien qu'une mesure visant à rendre les adresses URL imprévisibles puisse apparaitre adaptée et proportionnée en l'espèce, au regard du nombre de données à caractère personnel accessibles, de la nécessité de les protéger, et de la fragilité induite par l'existence d'adresses URL prévisibles, cette mesure ne présente effectivement pas un caractère obligatoire, d'autres mesures pouvant permettre d'assurer une protection équivalente des données traitées. Les précautions à prendre pour préserver la sécurité des données relèvent de la responsabilité du responsable de traitement.

La formation restreinte constate qu'en l'espèce, la société BOUYGUES TELECOM a fait le choix de ne pas mettre en œuvre de mesure complémentaire à l'authentification des utilisateurs du site web www.bouyguestelecom.fr. En conséquence, la formation restreinte estime que ce choix a fait peser sur la société une obligation particulièrement renforcée quant à la vigilance qu'il convenait de porter à cette unique mesure de sécurité.

(…) Si la formation restreinte constate que la société justifie de la réalisation de plusieurs tests d'intrusion et de plusieurs audits portant sur le code de son site web, elle relève que ces tests n'étaient pas adaptés aux spécificités de la base héritée et qu'ils ne pouvaient amener à la découverte de la vulnérabilité. Ces tests étaient donc inefficaces en l'espèce.

De la même manière, si la formation restreinte pourrait admettre qu'une revue manuelle de l'ensemble du code du site web de la société peut ne pas être proportionnée au regard du nombre de lignes composant ce code, la formation restreinte estime néanmoins que l'attention particulière à apporter au mécanisme d'authentification nécessitait une revue manuelle du code portant

uniquement sur cet élément critique. Une telle mesure n'apparaît en effet pas disproportionnée dans ce cas précis, tant au regard des moyens humaines et techniques à disposition de la société BOUYGUES TELECOM que des risques encourus par plus de deux millions de personnes concernées par la violation. »

3- Délibération de la formation restreinte n° SAN-2018-011 du 19 décembre 2018 prononçant une sanction pécuniaire à l'encontre de la société *Uber France SAS*

La formation restreinte de la CNIL a prononcé une sanction de 400.000 euros à l'encontre de la société UBER pour avoir fait preuve de négligence en ne mettant pas en place certaines mesures élémentaires de sécurité.

Elle considère que constitue une précaution élémentaire, la sécurisation de la connexion des serveurs utilisés par une entreprise. De plus, la mise en place d'un système de filtrage des adresses IP constitue un effort nécessaire devant être planifié dès le début de l'utilisation des services.

Faits - Le 21 novembre 2017, la société UBER TECHNOLOGIES INC. a publié sur son site internet un article faisant état de ce qu'à la fin de l'année 2016, deux individus extérieurs à la société avaient accédé aux données de 57 millions d'utilisateurs des services UBER à travers le monde. Cette information a ensuite été reprise dans de nombreux articles de presse dont certains faisaient état de ce que la société avait versé aux attaquants la somme de 100 000 dollars américains afin que ceux-ci détruisent les données en question et qu'ils ne révèlent pas l'existence de cet incident.

A l'issue de son instruction, le rapporteur a notifié à la société UBER FRANCE SAS le 6 août 2018, et communiqué pour information aux sociétés UBER B.V et UBER TECHNOLOGIES INC., un rapport détaillant les manquements à la loi qu'il estimait constitués en l'espèce et a proposé à la formation restreinte de la CNIL de prononcer une sanction pécuniaire de quatre cent mille (400.000) euros qui serait rendue publique

DELIBERATION (Extrait)

« (…) La formation restreinte relève que la plateforme GitHub étant utilisée par […], elle constituait un outil de travail central dans le développement des activités de la société, dont l'accès aurait dû être encadré par des règles de sécurité adéquates. En l'espèce, nonobstant la recommandation de la plateforme GitHub, il revenait bien à la société, en tant que responsable de traitement, d'adopter des règles à même de garantir la sécurité des informations stockées sur GitHub qui, si elles ne constituaient pas en elles-mêmes des données à caractère personnel (il s'agissait des clés d'accès aux serveurs […]), permettaient en revanche d'accéder directement à une grande quantité de données relatives aux utilisateurs du service UBER, puisque ces données étaient conservées sur les serveurs […].

(…) La formation restreinte considère que lorsque des collaborateurs sont amenés à se connecter à distance aux serveurs utilisés par une entreprise, la sécurisation de cette connexion constitue une précaution élémentaire afin de préserver la confidentialité des données traitées. Cette sécurisation peut, par exemple, reposer a minima sur la mise en place d'une mesure de filtrage des adresses IP afin que seules soient exécutées des requêtes provenant d'adresses IP identifiées, ce qui permet d'éviter toute connexion illicite, en sécurisant les échanges de données et en authentifiant les utilisateurs.

(…) Elle considère que compte tenu du nombre très important de personnes dont les données personnelles sont conservées les serveurs […], la mise en place d'un système de filtrage des adresses IP, quand bien même cela nécessitait un long développement, constituait un effort nécessaire qui aurait dû être planifié dès le début de l'utilisation des services […].[…]. »

III- Vidéosurveillance

Décision n° MED 2018-041 du 8 octobre 2018 mettant en demeure l'*Association « 42 »*

La CNIL met l'Association « 42 » en demeure de mettre en conformité avec la loi Informatique et Libertés son système de vidéosurveillance.

Faits - Dispositif de vidéosurveillance. – L'école 42 a installé des caméras de surveillance permettant de visualiser les espaces de travail des étudiants, les postes de travail des salariés, les espaces de pause et l'accès aux sanitaires. Le personnel administratif et les agents de sécurité ont accès à l'ensemble des images, sur des postes de travail protégés par un mot de passe de 5 caractères alphanumériques, les étudiants ont accès aux images des caméras visualisant les lieux qui leur sont accessibles. Le dispositif est mentionné dans le règlement intérieur et sur des autocollants placés sur les portes d'entrée de l'école.

DÉLIBÉRATION (Extrait)

« Gestion administrative des étudiants » – Les candidats à l'école doivent créer un compte sur le site de l'école avant de pouvoir passer les tests d'admissibilité. Le mot de passe de ces comptes sont générés automatiquement et envoyés en clair dans un courriel sans obligation de modification ni de renouvellement, et si le mot de passe est modifié celui-ci doit être composé de 8 caractères alphanumériques comprenant des lettres majuscules et minuscules. Aucune information relative au traitement des données n'est délivrée aux candidats. Les comptes créés par les candidats ne sont jamais supprimés et les données des étudiants sont conservées sans limite de temps. Dans la base de données dédiée à la gestion des étudiants, il a été constaté des commentaires tels que « diagnostiqué de plusieurs maladies graves » ou « très lourdement endetté. »

Un manquement à l'obligation de veiller à l'adéquation, à la pertinence et au caractère non excessif des données. – La CNIL autorise l'enregistrement en continu des accès de l'établissement et des espaces de circulation, mais la surveillance permanente des postes de travail des employés pendant les heures d'ouverture de l'établissement est prohibée, sauf circonstance particulière non démontrée en l'espèce. En outre, les commentaires relatifs à l'état de santé de l'étudiant ou à sa situation familiale sont disproportionnés au regard de la finalité du traitement, ici la gestion pédagogique de l'étudiant. Ces faits constituent un manquement au 3° de l'article 6 de la loi n°78-17 du 6 janvier 1978 modifiée.

Un manquement à l'obligation de définir une durée de conservation des données proportionnée à la finalité du traitement. – Les données à caractère personnel doivent être conservées uniquement le temps nécessaire à l'accomplissement de la finalité qui était poursuivie lors de leur collecte, et seules les données permettant l'identification des candidats peuvent être conservées. De plus, la conservation pour une durée indéfinie des comptes et des dossiers pédagogiques est disproportionnée à la finalité du traitement, en l'espèce l'analyse des parcours suivis au sein de l'école. Ces faits constituent un manquement à l'article 6-5 de la loi du 6 janvier 1978 modifiée.

Un manquement à l'obligation d'informer les personnes. – Les étudiants et les salariés ne sont pas informés des destinataires des données, de la durée de conservation des images enregistrées par

les caméras de vidéosurveillance ou du régime juridique applicable. Les personnes extérieures à l'établissement ne sont pas informées de l'identité du responsable du traitement, des destinataires, de la durée de conservation des images et des droits dont elles disposent. Aucune information relative au traitement de leurs données n'est fournie aux étudiants s'inscrivant sur le site internet de l'école. Ces faits constituent un manquement au I de l'article 32 de la loi n°78-17 du 6 janvier 1978 modifiée.

Un manquement à l'obligation d'assurer la sécurité et la confidentialité des données. – L'accès aux images issues du système de vidéosurveillance doit être strictement réservé aux personnes habilitées au regard de leur fonction. Permettre l'accès aux images à toute personne non habilitée compromet la confidentialité des données traitées. Un mot de passe insuffisamment complexe peut conduire à une compromission des comptes. Les mots de passe adressés aux étudiants dans un courriel en clair sans obligation de modification ont pour conséquence que les administrateurs de l'école connaîtront les mots de passe jamais modifiés. Ces faits constituent un manquement à l'article 34 de la loi n°78-17 du 6 janvier 1978 modifiée ».

IV- Détournement de finalité

Décision n° MED-2018-034 du 25 septembre 2018, *Malakoff-Médéric Mutuelle*

La CNIL a prononcé le 21 janvier 2019 une sanction de 50 millions d'euros à l'encontre de Google LLC en application du RGPD pour manque de transparence, information insatisfaisante et absence de consentement préalable.

Faits – L'AGIRC-ARRCO met en œuvre plusieurs traitements de données à caractère personnel rassemblés dans un système appelé « l'usine retraite. » L'AGIRC-ARRCO détermine les finalités et les moyens de ces traitements de données à caractère personnel. La société Malakoff Médéric Mutuelle a fait procéder à une campagne de prospection commerciale relative à la santé par courrier et par téléphone. La CNIL a constaté que tout ou partie des informations personnelles utilisées à l'occasion de ces campagnes de prospection commerciale (adresse postale et numéros de téléphone notamment) était issu de l'usine retraite.

DÉLIBÉRATION (Extrait)

« **L'identification du responsable du traitement. –** L'article 3 de la loi 78-17 du 6 janvier 1978 modifiée dans sa version en vigueur au 13 février 2018, jour du contrôle, dispose que « le responsable d'un traitement de données à caractère personnel est […] la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens. » En utilisant à des fins commerciales des données à caractère personnel qu'elle détient dans le cadre de sa mission d'intérêt général, la société Malakoff Médéric Mutuelle a déterminé de nouvelles finalités et de nouveaux moyens au traitement visé, et s'est comportée comme le responsable du traitement. Elle est donc, à ce titre, considérée comme tel.

Un manquement à l'interdiction de traiter ultérieurement, d'une manière incompatible avec la finalité initiale, des données collectées pour des finalités déterminées. – L'AGIRC-ARRCO n'a pas autorisé la société Malakoff Médéric Mutuelle à réutiliser les données à caractère personnel issues du système d'information de la retraite complémentaire. L'instruction AGIRC-ARRCO 2008/94 relative aux formalités déclaratives auprès de la CNIL précise que l'utilisation des applicatifs de l'usine retraite à d'autres fins que les besoins de gestion de la retraite complémentaire n'est pas envisageable. Cela a également été rappelé par les présidents de l'AGIRC-ARRCO dans leur lettre du 29 août 2017 aux présidents des groupes de protection sociale : conformément à la réglementation en vigueur, une utilisation des données personnelles de la retraite complémentaire

ne saurait être envisagée à d'autres fins que celle pour laquelle elles ont été initialement collectées sans l'accord individuel de chacune des personnes concernées. Ainsi, l'utilisation des données par la société Malakoff Médéric Mutuelle constitue un manquement au 2° de l'article 6 de la loi n°78-17 du 6 janvier 1978 modifiée ».

Internet et fraude informatique
Me Alexandre Bories, avocat au barreau de Montpellier

1- Cass. com. 28 mars 2018, n° 16-20018, *Comm. Com. Electr.*, mai 2018, com. 34, note G. Loiseau

La communication de données personnelles par l'utilisateur d'un service de paiement en réponse à un courriel, contenant des indices permettant à un utilisateur normalement attentif de douter de sa provenance (hameçonnage), constitue une négligence grave à l'obligation de garde et de conservation des données personnelles du dispositif de sécurité personnalisé de l'utilisateur. La banque n'a alors pas d'obligation de remboursement des sommes envers son client.

Faits - En l'espèce, M. Y, victime d'un hameçonnage, a renseigné précisément un « certificat de sécurité à remplir attentivement » en réponse à plusieurs courriels. Il a ensuite assigné sa banque en remboursement des sommes avec succès. Cette dernière se pourvoi en cassation en opposant une négligence grave de la part de son client.

ARRÊT (Extrait)

« Attendu que pour statuer comme il fait, l'arrêt, après avoir relevé que M. Y... a été victime d'un hameçonnage, ayant reçu des courriels successifs portant le logo parfaitement imité du Crédit mutuel accompagnés d'un "certificat de sécurité à remplir attentivement" qu'il a scrupuleusement renseignés, allant même jusqu'à demander à la banque la communication de sa nouvelle carte de clefs personnelle pour pouvoir renseigner complètement le certificat litigieux, ce qui montre sa totale naïveté, retient que la banque convient que seul un examen vigilant des adresses internet changeantes du correspondant ou certains indices, comme les fautes d'orthographe du message, sont de nature à interpeller le client, ce à quoi n'est pas nécessairement sensible un client non avisé, étant observé que M. Y..., qui ne se connectait quasiment jamais au site internet de la banque, ignorait les alertes de cette dernière sur le hameçonnage, puis en déduit que c'est à son insu que M. Y... a fourni les renseignements qui ont permis les opérations frauduleuses sur son compte et que n'est pas constitutive d'une négligence grave le fait pour un client "normalement" attentif de n'avoir pas perçu les indices propres à faire douter de la provenance des messages reçus ;

Qu'en statuant ainsi, alors que manque, par négligence grave, à son obligation de prendre toute mesure raisonnable pour préserver la sécurité de ses dispositifs de sécurité personnalisés l'utilisateur d'un service de paiement qui communique les données personnelles de ce dispositif de sécurité en réponse à un courriel qui contient des indices permettant à un utilisateur normalement attentif de douter de sa provenance, peu important qu'il soit, ou non, avisé des risques d'hameçonnage, la cour d'appel a violé les textes susvisés ».

Références Doctrinales :
- J. Lasserre-Capdeville, « Nouvelle solution remarquable en matière de phishing », *Gaz. Pal.* 2018, n° 17, p. 20.
- L. Costes, « Phishing : négligence fautive du client d'une banque pour avoir communiqué ses données personnelles », *Revue Lamy droit de l'immatériel,* 2018, n° 148, p. 34-35.
- D. Legeais, « Hameçonnage », *RTD com* 2018, n° 2, p. 436.
- N. Kilgus, « Responsabilité du porteur d'une carte bancaire en cas de phishing » *JCP* G, 2018, n°16, p. 778.

2- CA Paris, 15 sept. 2017 : *Comm. Com. Electr.,* févr. 2018, com. 16, note E.-A. Caprioli

La Cour d'appel retient qu'il n'y a pas délit d'accès ou maintien frauduleux dans un système de traitement automatisé de données (STAD) lorsque celui-ci est dénué de protection particulière et dont les données sont accessibles au public. Par ailleurs, l'extraction d'une partie substantielle d'une base de données sur un site internet, même non protégée, en violation des conditions générales d'utilisation, constitue une extraction frauduleuse des données contenues dans le STAD au regard de l'article 323-1 du Code pénal. L'extraction de données personnelles est réprimée par l'article 226- 16 et s. du Code pénal sanctionnant les atteintes aux données à caractère personnel contenues dans les STAD.

Faits - En l'espèce, un individu a extrait des données (fiches de clients) d'un site concurrent (Weezevent) afin de créer son propre site. Il a été relaxé par jugement de première instance (TGI Paris, 12e ch. Corr. 1, 20 juin 2016) pour les faits notamment d'accès et maintien frauduleux dans un système de traitement automatisé de données (art. 323-1 du Code pénal) et d'extraction frauduleuse des données dans un STAD (art 323-3 C. pén.).

ARRÊT (Extrait)

« M. X. s'est maintenu sur le site qui n'avait aucune protection particulière. Les données étaient accessibles au public. Il n'est pas davantage établi qu'il se soit maintenu frauduleusement sur le site de Weezevent. […]

L'utilisation de scripts ou robots visant à collecter et sélectionner les données notamment aux fins de savoir si le client était actif ou non sur le site Weezevent constitue un moyen déloyal et frauduleux pour avoir été recueilli à l'insu des personnes physiques titulaires des adresses électroniques. […]

Les données copiées et tirées du site Weezevent étaient certes accessibles au public mais par la façon automatisée et sélective de procéder, cela a entraîné l'extraction importante de 44 380 fichiers dont 7 779 étaient retrouvés sur le site de M. X... soit environ 16 % des données du site victime sachant que ces données ne pouvaient être extraites sans autorisation expresse de Y.... Or, M. X.... a agi à l'insu du directeur du site... par des moyens techniques conçus à cet effet par l'appelant. […]

Les conditions d'utilisation du site internet Weezevent mentionnent que "le contenu de Weezevent ne saurait être utilisé et exploité que par Wezevent et/ou ses licenciés et toute exploitation de celui-ci est constitutive, sauf accord exprès de Weezevent d'un acte de contrefaçon prohibé. Le contenu de Weezevent ne doit en aucun cas être téléchargé, copié, altéré, modifié, supprimé, distribué, transmis, diffusé, loué, vendu, concédé, exploité, en toute ou partie et de quelque manière que ce soit, sans l'accord exprès et écrit de Weezevent". M. X ne pouvait l'ignorer puisqu'il indique avoir lu les conditions d'utilisation. »

Références Doctrinales :
- E.-A. Caprioli, « Collecte de données personnelles non protégées et extraction frauduleuse », *Comm. Com. Electr.,* févr. 2018, comm.16.

3- CA Paris, 14 nov. 2017 : RLDI, janv. 2018/144, p. 39 et legalis.net

L'introduction d'un lien hypertexte dans un site internet afin de capter les ressources publicitaires engendrées par ce site ainsi que sa clientèle constitue une entrave au fonctionnement normal d'un STAD.

Faits - En l'espèce, le co-créateur d'un site internet a détourné à son profit la clientèle du site à travers un lien de redirection des internautes vers un nouveau site ainsi que les revenus publicitaires du site provenant de Google. La société victime a obtenu gain de cause en première instance qui a condamné le co-créateur pour des faits d'escroquerie, d'abus de confiance et d'entrave au fonctionnement normal du STAD.

ARRÊT (Extrait)

« […] l'introduction d'un lien hypertexte dans le site internet exploité par Up To Ten, alors que cette introduction n'avait d'autre fin que de capter à son profit, l'ensemble des ressources engendrées par la consultation du site par les internautes ; Qu'il a ainsi sciemment entravé en le faussant, le fonctionnement normal du système de traitement automatisé mis en œuvre par UpToTen ; Que l'infraction étant là encore constituée, le jugement sera confirmé sur la déclaration de culpabilité […] ».

4 - Cass. crim. 7 nov. 2017, n° 16-84918, Com. Com. Électr., avr. 2018, com. 31, note E.-A. Caprioli

La mise à disposition des internautes d'un protocole de communication textuelle instantané sur internet (Web Irc), qui permet d'avoir connaissance de modalités concrètes d'opérations d'un collectif de pirates informatiques à l'encontre d'opérateurs d'importance vitale qui ont pour but d'entraver le fonctionnement d'un service de traitement automatisé de données (STAD) lorsqu'elle est effectuée de manière consciente, est constitutive du délit d'entente en vue de la préparation d'entraves au bon fonctionnement de systèmes de traitement automatisé de données.

Faits - En avril 2011, le portail internet d'EDF a fait l'objet d'une attaque par « déni de service distribué » dans le cadre d'une offensive menée par l'organisation hacktiviste *Anonymous.* L'enquête permet d'établir l'identité du titulaire du serveur, M. Pierrick Y, ayant relayé les appels aux attaques informatiques. M Pierrick Y est poursuivi du chef de participation à des ententes établies en vue de la préparation d'entraves au bon fonctionnement de systèmes de traitement automatisé de données (STAD). Il lui a été reproché d'avoir proposé ses services de passerelle vers le canal dédié à cette opération baptisée *Greenrights*.

Il s'est défendu en prétendant n'être qu'un acteur de mise en relation et n'avoir agi que dans le but de favoriser un usage flexible et libre d'internet. Il a insisté sur le fait que les liens rattachés à *Anonymous* n'étaient pas les seuls accessibles par son serveur et qu'il ne maîtrisait pas l'utilisation que les internautes en faisaient.

En première instance, M Pierrick Y est renvoyé des fins de la poursuite par le tribunal correctionnel. Le ministère public relève appel de cette décision.

La cour d'appel de Paris condamne M Pierrick Y à une peine de deux mois d'emprisonnement assortis du sursis avec mise à l'épreuve pour participation à une entente établie en vue de la préparation d'une entrave au fonctionnement d'un système automatisé de données.

M. Pierrick Y forme un pourvoi en cassation le 30 juin 2016 contre l'arrêt de la cour d'appel de Paris. La chambre criminelle de la Cour de Cassation rejette le pourvoi.

ARRÊT (Extrait)

« (…) Attendu que pour dire établie la participation de M. Y... à une entente formée en vue de conduire des entraves par déni de service contre des distributeurs d'énergie, en particulier la société

EDF, l'arrêt retient la diffusion de l'adresse de son raccourcisseur d'url [...], dans des documents d'"Anonymous", plus d'un an auparavant, la mise à disposition des internautes, par M. Y..., d'un web[...]dont il est locataire et gestionnaire, passerelle technique au fonctionnement simplifié permettant à ses usagers, en particulier non férus d'informatique, d'accéder à des sites de discussion, d'avoir connaissance des modalités concrètes d'opérations du mouvement "Anonymous", le terme "anonops" étant un raccourci des termes "anonymous" et "opérations", et l'intitulé "greenrights" visant les sujets ciblés par le mouvement ; que les juges ajoutent que le prévenu avait constaté qu'EDF était une cible du mouvement, dans le cadre des positions contre le nucléaire, et n'ignorait pas qu'un des moyens d'action des Anonymous était les entraves par déni de service et que la mise à disposition des moyens techniques et des informations, pour laquelle il avait obtenu le statut de "semi-opérateur", permettait de réaliser ces dénis de service ; que les juges en déduisent la pleine conscience qu'avait l'intéressé du caractère irrégulier de telles attaques, qu'il reconnaissait finalement désapprouver ;

Attendu qu'en statuant par des motifs qui établissent que le prévenu avait conscience de participer à une entente ayant pour but d'entraver le fonctionnement d'un service de traitement automatisé de données, la cour d'appel, qui n'a méconnu aucun des textes visés au moyen, a justifié sa décision ; (...) ».

Références Doctrinales :
- W. Azoulay, « Déni de service distribué et passerelle en ligne : l'organisation d'une bande désorganisée » *Dalloz actualité*, 24 nov. 2017.
- J.B. Thierry, « Participation à une cyber-association de malfaiteurs » *AJ Pénal* 2018, p. 44
- E. Dreyer, *«* Association de malfaiteurs en vue de porter atteinte à un STAD*», RSC 2018* p.114
- E.-A. Caprioli, « Entente ayant pour but d'entraver le fonctionnement d'un STAD », *Comm. Com. Elect.,* avr. 2018, comm.31

5 - Cass. crim. 27 mars 2018, n° 17-81989 : Comm. Com. Electr., juillet-août 2018, com. 59, note E.-A. Caprioli

L'accès peut être frauduleux même sans utilisation d'un procédé quelconque : utiliser un ordinateur laissé allumer par son propriétaire, à l'insu de celui-ci, pour vérifier le contenu de son disque dur, constitue une infraction.

Faits : Le 12 novembre 2014 M. Frédéric X envoie des mails sous un faux nom sur l'adresse professionnelle du conjoint de la plaignante, Mme Régine C., faisant allusions à des rapports intimes entre M.X et Mme. C, dans le but de faire croire à son mari que celle-ci le trompait. Le 9 décembre 2014, M.X admet être l'auteur des mails et indique qu'il a récupéré dans la boîte email de Mme Régine C, sur l'ordinateur professionnel de celle-ci, d'une part, un échange email intime et, d'autre part, l'adresse professionnelle du conjoint de la plaignante. Une plainte est déposée contre M. Frédéric X pour des faits d'harcèlement sexuel et d'intrusion dans un système de traitement automatisé de données.

L'ordinateur n'était protégé par un code qu'à l'issue d'une période d'inactivité. M. X affirme qu'il n'a pas forcé ni utilisé aucun code pour examiner la boite mail de l'ordinateur qui était selon lui allumé.

Le tribunal correctionnel renvoie M.X des fins de la poursuite.

La partie civile relève appel. Le 13 février 2017, la cour d'appel de Rouen infirme le jugement et condamne M. Frédéric X à trois mois d'emprisonnement avec sursis pour accès et maintien frauduleux dans un système de traitement automatisé de données.

Le prévenu forme un pourvoi. La chambre criminelle de la cour de Cassation rejette le pourvoi.

ARRÊT (Extrait)

« (…) Attendu que, pour infirmer le jugement sur l'action publique, l'arrêt énonce que le prévenu, s'il affirme n'avoir forcé ni utilisé aucun code, a accédé volontairement, à l'insu de la partie civile, à la messagerie électronique de celle-ci accessible depuis son ordinateur professionnel, qui n'était protégé par un code qu'à l'issue d'une période d'inactivité, au contenu et à la copie de messages qui y étaient stockés, et ce dans le but de lui nuire ; (…)

(…) Attendu qu'en l'état de ces énonciations, relevant de son appréciation souveraine des faits de la cause, la cour d'appel a justifié sa décision, dès lors que se rend coupable de l'infraction prévue à l'article 323-1 du code pénal la personne qui, sachant qu'elle n'y est pas autorisée, accède par quelque moyen que ce soit à un système de traitement automatisé de données ; (...) ».

6- Cass. crim. 16 janv. 2018, n° 16-87168, *Comm. Com. Electr.,* avr. 2018, com. 30, note E.-A. Caprioli

Se rend coupable de l'infraction prévue à l'article 323-1 du code pénal la personne qui détient et installe un keylogger sur des ordinateurs, pour intercepter à l'insu de leurs utilisateurs, par l'espionnage de la frappe du clavier, les codes d'accès et accéder ainsi aux courriels.

Faits : Le 12 novembre 2013, le service informatique du CHU de Nice a découvert qu'un keylogger - dispositif permettant d'espionner la frappe du clavier et de capter des données - avait été installé sur les ordinateurs de deux praticiens hospitaliers titulaires.

Après enquête, des poursuites sont lancées à l'encontre de M. Romain Y pour accès frauduleux à tout ou partie d'un système de traitement automatisé de données, atteinte au secret des correspondances émises par voie électronique et détention sans motif légitime d'équipement, d'instrument de programme ou données conçus ou adaptés pour une atteinte au fonctionnement d'un système de traitement automatisé.

M. Y est condamné en première instance. Il interjette appel.

Le 8 novembre 2016, la cour d'appel d'Aix-en Provence confirme le jugement de première instance. M. Romain Y forme un pourvoi. La chambre criminelle de la cour de Cassation rejette le pourvoi.

ARRÊT (Extrait)

« (…) Attendu que, pour dire établis les délits reprochés, l'arrêt retient que la détention d'un keylogger, sans motif légitime, par M. Y..., que celui-ci ne conteste pas avoir installé sur l'ordinateur des docteurs E… et C..., pour intercepter à leur insu, par l'espionnage de la frappe du clavier, les codes d'accès et accéder aux courriels échangés par les deux praticiens caractérisent suffisamment sa mauvaise foi et les délits tant dans leur élément matériel qu'intentionnel ; que les juges ajoutent que les motifs avancés par le prévenu pour justifier la détention d'un équipement conçu ou adapté pour une atteinte frauduleuse à un système de traitement automatisé de données, à savoir la défense de sa situation professionnelle et sa réputation, sont indifférents à la caractérisation des infractions, puisque l'autorisation de détention prévue par l'article 323-3-1 du code pénal, autorisant un tel équipement, se limite aux seules personnes habilitées à assurer la maintenance et la sécurité d'un parc informatique ;

Attendu qu'en l'état de ces énonciations, relevant de son appréciation souveraine des faits de la cause, la cour d'appel a justifié sa décision ; qu'en effet, se rend coupable de l'infraction prévue à l'article 323-1 du code pénal la personne qui, sachant qu'elle n'y est pas autorisée, accède, à l'insu des victimes, à un système de traitement automatisé de données ;

D'où il suit que le moyen ne saurait être accueilli ; (…) ».

Références Doctrinales :
- E. Dreyer, « Accès frauduleux, indirect, mais certain, dans un STAD et détention du matériel le permettant », *RSC 2018*, p. 701.
- G. Roujou de Boubée, T. Garé, C. Ginestet, S. Mirabail, E. Tricoire, « Droit pénal », *Dalloz* 2018, p. 2259.
- P. Mistretta, « Le secret des correspondances, Molière et les tartufferies médicales… », *RSC 2018*, p. 480.
- E.-A. Caprioli, « Usage frauduleux d'un logiciel keylogger », *Communication Commerce Electronique.*, avr. 2018, comm. 30.

Internet et relations de travail

Me Axel Saint-Martin, avocat au barreau de Montpellier

1- CEDH, 5° sect. 22 févr. 2018, n° 588/13

2- Cass. soc. 13 juin 2018, n° 16-17865

3- Cass. soc. 12 sept. 2018, n° 16-11690

Les décisions sont commentées à la *Chronique Droit de l'internet de l'ERCIM* (*JCP* E 2019 du 31 janvier 2019, n° 5, Chron. 1043). Merci de vous y reporter.