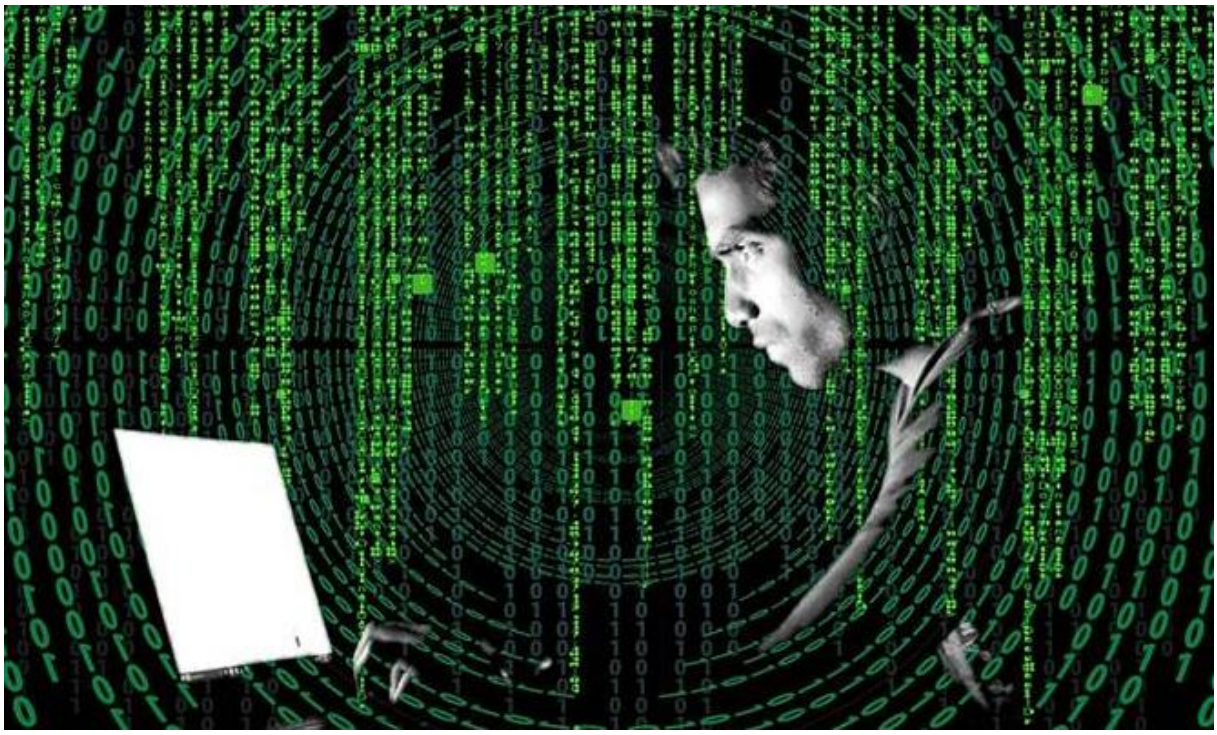
LEX CONTRACTUS

contact@lexcontractus.fr - 05 56 44 40 56
12 avenue de Tivoli - 33110 Le Bouscat

ACTUALITÉS OCTOBRE 2019

DROIT DU NUMÉRIQUE



Rédacteur :

Maître Cédric BERNAT
Docteur en Droit – Avocat
Membre de l'IDABB (Institut de Droit des Affaires du Barreau de Bordeaux)
Membre de l'AFDM (Association Française du Droit Maritime)

Première partie.
ACTUALITÉ JURISPRUDENTIELLE

1. FAILLES DANS LA SÉCURISATION DES DONNÉES ACCESSIBLES « EN LIGNE » : CONTRÔLE ET SANCTION DE LA CNIL[1] – ET CONTRÔLE DES DÉCISIONS DE LA CNIL, PAR LE JUGE

Conseil d'Etat, 9ème et 10ème Chambres réunies, 17 avril 2019
Décision n° 422575, publiée au Recueil Lebon

Le 31 juillet 2017, une délégation de la CNIL a effectué des vérifications en ligne sur le site de la société OPTICAL CENTER, qui ont permis de constater qu'il était **possible d'accéder librement**, à partir des URL qui lui avaient été transmises, **à des factures contenant les données à caractère personnel** suivantes : le nom, le prénom, l'adresse postale, la correction ophtalmologique et, pour certaines d'entre elles, la date de naissance des clients ainsi que leur numéro d'inscription au répertoire national d'identification des personnes physiques (NIR).
La délégation a également constaté qu'il était possible, depuis le domaine « optical-center.fr » et sans authentification préalable dans l'espace client, d'exporter au format « CSV », un échantillon de 2085 fichiers correspondant, après suppression des doublons, aux **données de 1207 clients** et faisant notamment apparaître 158 NIR.
L'alerte ayant été donnée le jour même par la CNIL à la société OPTICAL CENTER, celle-ci a déclaré avoir corrigé avec son prestataire, dès le 2 août 2017, le défaut de sécurité affectant son site.
Lors d'un contrôle sur place effectué le 9 août 2017, la délégation de la CNIL a constaté l'adjonction d'une fonctionnalité permettant de s'assurer qu'un client est effectivement connecté à son espace personnel avant de lui fournir les seuls documents le concernant.
Par une délibération du 7 mai 2018, la formation restreinte de la CNIL a prononcé à l'encontre de la société OPTICAL CENTER, une sanction pécuniaire d'un montant de 250 000 euros et a rendu sa décision publique pendant une durée de 2 ans à compter de sa publication.

Le 25 juillet 2018, la société OPTICAL CENTER a formé un recours devant le Conseil d'Etat.

Par décision du 17 AVRIL 2019, le Conseil d'Etat a censuré (partiellement) la décision de la CNIL. L'arrêt du Conseil d'Etat s'articule en trois points.

1°) Contrôle de légalité de la procédure de sanction

Le Conseil d'Etat a rappelé qu'en application des dispositions de l'article 45, § I, de la loi du 6 janvier 1978 (modifiée, relative à l'informatique, aux fichiers et aux libertés, dans sa rédaction applicable au litige issue de la loi du 7 octobre 2016 pour une République numérique), que la formation restreinte de la CNIL peut, sans mise en demeure préalable, sanctionner un responsable de traitement dont les manquements aux obligations qui lui incombent ne sont pas susceptibles d'être régularisés, soit qu'ils soient insusceptibles de l'être, soit qu'il y ait déjà été remédié.

En l'espèce, le Conseil d'Etat estime qu'à la suite d'une mesure correctrice apportée le 2 août 2017, le manquement aux obligations de sécurité constaté par la mission de contrôle de la CNIL avait cessé et n'était dès lors plus susceptible de faire l'objet d'une régularisation. Il

[1] Commission Nationale de l'Informatique et des Libertés, créée par la loi informatique et libertés du 6 janvier 1978.

s'ensuit que c'est à bon droit que la formation restreinte de la CNIL a pu légalement, engager, sans procéder à une mise en demeure préalable, une procédure de sanction, à l'encontre de la société OPTICAL CENTER.

2°) Contrôle de la caractérisation de l'existence d'un manquement aux obligations légales de sécurité

Le Conseil d'Etat rappelle qu'en application de l'article 34 de cette même loi de 1978 : « Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ».

En l'espèce :
◆ La haute juridiction administrative constate qu'il résulte de l'instruction, qu'avant sa mise en conformité à la suite de l'intervention de la CNIL, **le site internet** de la société OPTICAL CENTER, qui permet d'effectuer des commandes en ligne après avoir créé un compte dédié, **n'intégrait pas de fonctionnalité permettant de vérifier** qu'un client s'était bien authentifié à son espace personnel **avant de lui donner accès** à ses factures et bons de commande, lesquels pouvaient inclure des **données sensibles**, telles des données de santé ou des numéros NIR.
L'ensemble des données concernées, dans une base d'au moins 334769 documents, étaient donc **accessibles sans contrôle préalable** et sans qu'il soit besoin d'une maîtrise technique particulière, à tout client par la simple modification, lors de la consultation d'une facture ou d'un bon de commande, du paramètre « id », très visible, relatif à l'identifiant de la facture.
◆ De plus, il ne résulte pas de l'instruction, que la société OPTICAL CENTER aurait pris des **précautions de sécurité suffisantes en mettant en place un protocole** de tests **en amont de la mise en production de son site internet** en décembre 2016 **ou en établissant un programme d'audits de sécurité ultérieurs**.
Le Conseil d'Etat en déduit que c'est à bon droit que la formation restreinte de la CNIL a caractérisé l'existence d'un manquement aux obligations de sécurité prévues par l'article 34 de la loi de 1978.

3°) Contrôle du caractère proportionné de la sanction pécuniaire, au regard de la célérité à remédier aux manquements constatés

Le Conseil d'Etat rappelle, qu'en application de l'article 47 de la loi du 6 janvier 1978, lorsque la CNIL constate des manquements à l'obligation d'assurer la sécurité et la confidentialité des données, il lui appartient, pour prononcer une sanction, sous le contrôle du juge, de tenir compte de la nature, de la gravité et de la durée de ces manquements, mais aussi du comportement du responsable du traitement à la suite de ce constat.
C'est sur ce point que le Conseil d'Etat réforme partiellement la décision de la CNIL, au motif qu'en retenant une sanction pécuniaire d'un montant de 250 000 euros sans prendre en compte la célérité avec laquelle la société OPTICAL CENTER a apporté les mesures correctrices de nature à remédier aux manquements constatés, la formation restreinte de la CNIL a infligé à cette société une **sanction disproportionnée**.
Le Conseil d'Etat estime, par suite, qu'il sera fait une juste appréciation des circonstances de l'espèce, en ramenant cette sanction pécuniaire à un montant de 200 000 euros.

Mots Clé : Loi n° 78-17 du 6 janvier 1978 – Loi n° 2016-1321 du 7 octobre 2016 – Sécurité des données accessibles en ligne – Sécurisation d'un site internet – Formation restreinte de la CNIL – Responsabilité du Responsable du traitement des données (oui) – Manquements susceptibles d'être régularisés (non) – mise en demeure préalable par la CNIL (non) –

contrôles préalables à l'accès aux données – précautions de sécurité en amont de la mise en production du site internet ou programme d'audits de mise en sécurité ultérieurs - Sanction pécuniaire – Disproportion de la sanction au regard de la célérité à remédier aux manquements constatés

2. SANCTION D'UN COURTIER D'ASSURANCE POUR MANQUEMENT À SON OBLIGATION D'ASSURER LA CONFIDENTIALITÉ ET LA SECURITÉ DES DONNÉES A CARACTÈRE PERSONNEL TRAITÉES

CNIL – Formation restreinte – Décision du 18 juillet 2019
Décision n° SAN-2019-007

La société ACTIVE ASSURANCES (ci-après, la société AA) a une activité d'intermédiaire en assurance, concepteur et distributeur de contrats d'assurance automobile à des particuliers, en vente directe ou en vente en ligne. La société emploie environ 160 salariés, dont 150 sont situés à Madagascar au sein d'une succursale de la société. Pour les besoins de son activité, la société édite un site web, sur lequel les personnes peuvent demander des devis ou souscrire des contrats d'assurance automobile. La société obtient des clients, majoritairement via son site web, et par le biais de comparateurs d'assurances automobiles disponibles sur d'autres sites web.

Le 1er juin 2018, la CNIL a été informée, par un client de la société AA, qu'il avait accès aux données d'autres clients sans procédure d'authentification préalable. Le 27 juin suivant, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a également avisé la CNIL que l'accès aux données à caractère personnel des utilisateurs du site web de la société était possible sans contrôle préalable depuis le moteur de recherche Duckduckgo.

La mission de contrôle diligentée par la CNIL a constaté qu'une requête effectuée au sein du moteur de recherche Duckduckgo à partir des mots clés client.activeassurances.fr site:client.activeassurances.fr faisait apparaître des liens hypertextes permettant d'**accéder librement à certains comptes de clients de la société, sans authentification préalable**. En cliquant sur ces liens, la délégation a pu accéder à des comptes de clients - comportant notamment leur nom, prénom, adresse postale, adresse électronique, numéro de téléphone - et télécharger plusieurs documents PDF concernant des personnes, tels que des pièces d'identité, des devis, des attestations d'assurance automobile ou encore des contrats d'assurance. La délégation a également constaté que la modification du numéro identifiant apparaissant à la fin d'une des adresses URL affichées dans les résultats de recherche du moteur de recherche Duckduckgo permettait d'accéder aux comptes personnels d'autres clients de la société.

La société a été informée par téléphone le même jour, par la délégation, de l'existence d'un défaut de sécurité sur son site. Un courrier électronique contenant le type d'adresses URL concernées lui a également été adressé. Il était demandé à la société de prendre les mesures correctives nécessaires pour y remédier dans les plus brefs délais afin d'éviter tout accès aux données personnelles par des tiers non autorisés.

Par courrier du 2 juillet 2018, la société a indiqué à la Commission, par l'intermédiaire de son conseil, que plusieurs mesures avaient été prises afin de remédier au défaut de sécurité.

Le 12 juillet suivant, lors de la mission de contrôle dans les locaux de la société, cette dernière a informé la délégation qu'elle avait pris des mesures dès le 29 juin afin que les documents de ses clients ne soient plus accessibles à des tiers non autorisés.

À l'issue de son instruction, le rapporteur de la CNIL a fait notifier à la société AA, le 5 avril 2019, un rapport détaillant le manquement relatif à l'article 32 du RGPD qu'il estimait constitué en l'espèce. Ce **rapport proposait** à la formation restreinte de la CNIL de prononcer à l'encontre de la société AA, une **amende administrative** d'un montant de **375 000 euros** et qui serait rendue publique.

Dans sa délibération du 18 juillet 2019, la formation restreinte de la CNIL prononce une **sanction de 180 000 euros**, au visa de l'article 32 du RGPD, et ordonne la publication de la décision, aux motifs suivants :

1°) Sur le manquement à l'obligation d'assurer la sécurité et la confidentialité des données à caractère personnel

En l'espèce, le manquement est double.

► Sur le défaut de sécurité ayant entraîné la violation de données à caractère personnel

◆ Tout en soulignant la diligence de la société qui a réagi rapidement après la révélation de l'incident pour le corriger, la formation restreinte relève que les mesures élémentaires de sécurité n'avaient pas été prises en amont du développement de son site web, ce qui a rendu possible la survenance de la violation de données à caractère personnel.

La formation restreinte estime que la violation de données à caractère personnel résultant de ce défaut de sécurité aurait pu être évitée si, par exemple, la société avait mis en œuvre une mesure d'authentification et une gestion des droits d'accès permettant de s'assurer que chaque utilisateur souhaitant accéder à un document était habilité à le consulter.

Elle considère que ce défaut de sécurité démontre que, **dès sa conception en 2014, le site web de la société était défectueux** et que celle-ci **n'avait pas mis en place les mesures appropriées et élémentaires de sécurité**.

De plus, le défaut de sécurité a été amplifié par le fait que les documents des personnes, librement accessibles depuis le site web de la société, ont été indexés par les moteurs de recherche Duckduckgo, Bing, Qwant et Yahoo. Cette indexation a été rendue possible dès lors que **la société n'avait pas mis en place de mesures** permettant de limiter celle-ci par les moteurs de recherche, au moyen, par exemple, d'un fichier robot.txt.

Par ailleurs, la formation restreinte estime que la société aurait dû mettre en place ces mesures élémentaires qui ne nécessitaient pas de développements techniques importants.

La société n'a pas mis en œuvre les mesures techniques et organisationnelles appropriées afin de garantir la sécurité des données personnelles traitées, conformément à l'article 32 du Règlement.

◆ La formation restreinte constate que la société a mis en place les mesures correctives nécessaires à la sécurisation des données à caractère personnel et prend acte du fait qu'un plan de remédiation plus général, permettant d'assurer sa conformité avec la règlementation, a été déterminé.

Cependant, la formation restreinte relève que la résolution du défaut de sécurité n'a pu être effectuée qu'à la faveur d'un signalement d'un client de la société qui a tenté en vain de l'en informer en mai 2018. En outre, les mesures élémentaires nécessaires à la sécurisation des données de ses clients n'ont été mises en place par la société qu'après le signalement puis l'intervention des services de la Commission auprès de celle-ci.
La formation restreinte considère dès lors que la société n'a placé la sécurité des données de ses clients au cœur de ses préoccupations qu'après l'intervention des services de la Commission.

◆ En second lieu, en ce qui concerne le nombre de personnes concernées par le défaut de sécurité, la formation restreinte relève que la délégation a constaté, lors du contrôle sur place, que la base contenait 148 359 numéros de téléphone distincts et 144 057 adresses électroniques distinctes concernant des clients. La société a précisé, à cette occasion, que les données personnelles et pièces justificatives relatives à tous les contrats conclus par la société, résiliés ou non, étaient librement accessibles en raison du défaut de sécurité constaté.

En outre, un grand nombre de documents étaient rendus **accessibles du fait du défaut de sécurité** affectant le site web de la société, à savoir notamment **144 890 copies de carte grise, 137 776 copies de permis de conduire, 119 940 relevés d'identité bancaire, 119 517 devis ou encore 36 068 copies de déclarations de cession d'un véhicule**.
Chaque document contient, de par sa nature, de multiples informations sur la personne concernée telles que ses nom, prénom, adresse postale, adresse électronique, date et lieu de naissance, coordonnées bancaires, immatriculation du véhicule ou encore des éléments relatifs à la suspension du permis de conduire et les motifs de résiliation de garantie de la part de la société.
Par conséquent, le défaut de sécurité a concerné un nombre particulièrement important de données à caractère personnel et de documents concernant les clients de la société.

De plus, la formation restreinte relève que le défaut de sécurité a concerné des documents contenant des éléments permettant de révéler des informations particulièrement précises sur les personnes. Il était ainsi possible d'avoir accès à l'historique des clients en matière d'assurance automobile et de savoir ainsi si une personne avait fait l'objet d'une résiliation ou d'une annulation de contrat pour fausse déclaration ou pour non-paiement d'une prime, ou encore si elle avait fait l'objet d'un retrait de permis ou commis un délit de fuite ou un refus d'obtempérer.

Sur ce dernier point, la formation restreinte relève que les données en question sont relatives à des infractions commises par les personnes et aux suites qui leur ont été données. Elle rappelle que le considérant 83 du RGPD prévoit que les mesures permettant d'atténuer les risques inhérents au traitement doivent assurer un niveau de sécurité approprié, y compris la confidentialité, compte tenu de l'état des connaissances et des coûts de mise en œuvre par rapport aux risques et à la nature des données à caractère personnel à protéger. Par conséquent, **de telles données, considérées comment étant des données particulières, doivent faire l'objet de la part des responsables de traitement d'une vigilance et d'une protection renforcées, ce qui n'a pas été le cas en l'espèce**.

► Sur l'absence de robustesse des mots de passe d'accès aux comptes clients de la société

La délégation de la CNIL a constaté que les clients devaient se connecter à leur espace personnel accessible en ligne, via leur numéro client et leur date de naissance, cette seconde information valant mot de passe. La société a informé la délégation qu'aucune mesure complémentaire pour l'authentification des personnes, telle qu'une limitation du nombre de tentatives en cas de mots de passe erronés, n'avait été mise en place.

La formation restreinte rappelle que, **pour assurer un niveau de sécurité suffisant et satisfaire aux exigences de robustesse des mots de passe**, lorsqu'une authentification repose uniquement sur un identifiant et un mot de passe, **le mot de passe doit comporter au minimum** douze caractères - contenant au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial - ou le mot de passe doit comporter au moins huit caractères - contenant trois de ces quatre catégories de caractères - **et être accompagné d'une mesure complémentaire** comme par exemple la **temporisation d'accès au compte après plusieurs échecs** (suspension temporaire de l'accès dont la durée augmente à mesure des tentatives), la mise en place d'un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (ex : captcha) et/ou le blocage du compte après plusieurs tentatives d'authentification infructueuses.

La formation restreinte relève que la **nécessité d'un mot de passe fort** est également soulignée par l'ANSSI, qui indique qu'« *un bon mot de passe est avant tout un mot de passe fort, c'est à dire difficile à retrouver même à l'aide d'outils automatisés. La force d'un mot de passe dépend de sa longueur et du nombre de possibilités existantes pour chaque caractère le composant. En effet, un mot de passe constitué de minuscules, de majuscules, de caractères spéciaux et de chiffres est techniquement plus difficile à découvrir qu'un mot de passe constitué uniquement de minuscules* ».

En outre, il ressort des constats effectués, que le formulaire de connexion des clients à leur espace personnel indiquait expressément le format des mots de passe de connexion, à savoir la date de naissance des personnes, ce qui facilitait considérablement une attaque par force brute, ce d'autant que le format des mots de passe était indiqué sur le formulaire de connexion au compte client. La formation restreinte relève également que les clients désirant renforcer la sécurité de leurs données et modifier leur mot de passe en étaient empêchés par la société qui avait imposé le format relatif à la date de naissance.
La formation restreinte considère, par conséquent, que **les mots de passe mis en place par la société pour accéder aux comptes clients ne correspondaient pas aux exigences requises en termes de robustesse**.

Enfin, en ce qui concerne la **transmission des mots de passe aux clients** de la société par courriel, en clair, après la création du compte, la formation restreinte relève qu'une telle procédure ne permet pas d'assurer la sécurité des données, dès lors que l'envoi d'un courriel non chiffré peut conduire à son interception par toute personne écoutant le réseau et à la prise de connaissance des informations qu'il contient.

La société **a donc méconnu une mesure de sécurité élémentaire préconisée par la CNIL** alors que **la transmission des mots de passe en clair dans un courriel le rend accessible à tout tiers susceptible d'accéder à la messagerie électronique de la personne** concernée.
Le manquement à l'article 32 du Règlement est constitué.

2°) Sur la sanction et la publicité

Tout d'abord, la CNIL considère qu'en l'espèce, **les manquements précités justifient que soit prononcée une amende administrative à l'encontre de la société** pour les motifs suivants.

Elle rappelle que face aux risques représentés par les violations de données à caractère personnel, le législateur européen a entendu renforcer les obligations des responsables de traitement en matière de sécurité des traitements. Ainsi, selon le considérant 83 du RGPD, « *afin de garantir la sécurité et de prévenir tout traitement effectué en violation du présent Règlement, il importe que le responsable du traitement ou le sous-traitant évalue les risques inhérents au traitement et mette en œuvre des mesures pour les atténuer, telles que le chiffrement. Ces mesures devraient assurer un niveau de sécurité approprié, y compris la confidentialité, compte tenu de l'état des connaissances et des coûts de mise en œuvre par rapport aux risques et à la nature des données à caractère personnel à protéger. Dans le cadre de l'évaluation des risques pour la sécurité des données, il convient de prendre en compte les risques que présente le traitement de données à caractère personnel, tels que la destruction, la perte ou l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite, qui sont susceptibles d'entraîner des dommages physiques, matériels ou un préjudice moral* ». Or, la formation restreinte observe que la société n'a pas mesuré, avant d'être alertée par les services de la CNIL, l'importance de la sécurisation des données personnelles contenues dans ses systèmes d'information, malgré la nature des données traitées.

Ensuite, la CNIL considère que **la gravité du manquement est caractérisée** en l'espèce :
- en raison de la nature des données personnelles concernées, la société traitant des données particulièrement identifiantes, ainsi que des données relatives à des infractions,
- en raison du nombre de documents et de personnes concernées par le défaut de sécurité, celui-ci ayant affecté les comptes de plusieurs milliers de clients et de personnes ayant résilié leur contrat avec la société.

La formation restreinte rappelle, par ailleurs, que **le défaut de sécurité est dû à une conception défectueuse de son site web par la société, développé en 2014, et qu'il a donc perduré pendant plusieurs années**. En outre, la mise en œuvre d'une procédure d'authentification sur le site ainsi que celle d'une directive limitant l'indexation par les moteurs de recherche de certaines parties du site web étaient des mesures élémentaires.

Enfin, la formation restreinte relève que les décisions de sanction invoquées par la société ont été adoptées sous l'empire de la loi Informatique et Libertés telle que modifiée par la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, qui prévoyait que le montant de sanctions pouvant être prononcées par la formation restreinte ne pouvait excéder 3 millions d'euros. Les faits de l'espèce ont, eux, été constatés alors que le RGPD était entré en application et que le manquement constaté est susceptible de donner lieu à une amende pouvant s'élever jusqu'à 10 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 2% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

Toutefois, que la société a réagi rapidement après avoir eu connaissance de la violation de données en mettant en place des **mesures correctrices vingt-quatre heures après avoir été alertée par les services de la CNIL**. Elle prend également acte de ce que la société a coopéré avec la CNIL dans le cadre des différents échanges entretenus avec ses services à la suite des contrôles et de sa bonne foi dans la résolution du défaut de sécurité.
Elle relève enfin que la société a informé ses clients de la survenance du défaut de sécurité et qu'aucun dommage les concernant n'a été porté à sa connaissance.

Compte tenu de l'ensemble de ces éléments, la formation restreinte, tenant compte des critères fixés à l'article 83 du RGPD, estime qu'**une amende administrative à hauteur de 180 000 euros est justifiée et proportionnée**, ainsi qu'une **sanction complémentaire de publicité** pour les mêmes motifs.

Pour mémoire, la formation restreinte de la CNIL a motivé sa décision de sanction du 18 juillet 2019, au visa des deux textes suivants :

► L'article 20-III de la loi du 6 janvier 1978, modifiée : « *Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut également, le cas échéant après lui avoir adressé l'avertissement prévu au I du présent article ou, le cas échéant en complément d'une mise en demeure prévue au II, saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes:*
[…]
7° À l'exception des cas où le traitement est mis en œuvre par l'État, une amende administrative ne pouvant excéder 10 millions d'euros ou, s'agissant d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Dans les hypothèses mentionnées aux 5 et 6 de l'article 83 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, ces plafonds sont portés, respectivement, à 20 millions d'euros et 4 % dudit chiffre d'affaires. La formation

restreinte prend en compte, dans la détermination du montant de l'amende, les critères précisés au même article 83 ».

► L'article 83 du RGPD : « *Chaque autorité de contrôle veille à ce que les* ***amendes administratives*** *imposées en vertu du présent article pour des violations du présent règlement, visées aux paragraphes 4, 5 et 6 soient, dans chaque cas,* ***effectives, proportionnées et dissuasives****. Selon les caractéristiques propres à chaque cas, les amendes administratives sont imposées en complément ou à la place des mesures visées à l'article 58, paragraphe 2, points a) à h), et j). Pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative, il est dûment tenu compte, dans chaque cas d'espèce, des éléments suivants :*
a) la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi ;
b) le fait que la violation a été commise délibérément ou par négligence ;
c) toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées ;
d) le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre en vertu des articles 25 et 32 ;
e) toute violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant ;
f) le degré de coopération établi avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs ;
g) les catégories de données à caractère personnel concernées par la violation ;
h) la manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure, le responsable du traitement ou le sous-traitant a notifié la violation ;
i) lorsque des mesures visées à l'article 58, paragraphe 2, ont été précédemment ordonnées à l'encontre du responsable du traitement ou du sous-traitant concerné pour le même objet, le respect de ces mesures ;
j) l'application de codes de conduite approuvés en application de l'article 40 ou de mécanismes de certification approuvés en application de l'article 42 ;
et k) toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation ».

Mots Clé : Article 20-III de la loi du 6 janvier 1978 - Article 32 du RGPD – Article 83 du RGPD – Sécurité et la confidentialité des données à caractère personnel : manquement (oui) – Site web défectueux dès sa conception (oui) – Absence de mise en place les mesures appropriées et élémentaires de sécurité (oui) – Protection renforcée des données sensibles – Absence de robustesse des mots de passe d'accès aux comptes clients de la société – Modalités de transmission sécurisée des mots de passe – Communication des mots de passe par simple emails : défaut de sécurité élémentaire sanctionnable – Sanction de la CNIL (oui) – Amende administrative – Amende effective, proportionnée et dissuasive (oui) – Sanction complémentaire de publicité (oui).

Deuxième partie.

MISES EN DEMEURE DE LA CNIL RENDUES PUBLIQUES (Second semestre 2018)

La CNIL a récemment adressé des mises en demeure, à quatre sociétés, pour mettre un terme au plus vite, à des **pratiques de profilage et ciblage publicitaire par géolocalisation**, qu'elle estime contraire :

- aux dispositions de la loi du 6 janvier 1978 (LIL – loi informatique et libertés),
- et au règlement européen dit RGPD (règlement général de la protection des données) du 27 avril 2016, entré en vigueur le 25 mai 2018 :

◆ Mise en demeure n° 2018-022 du 25 juin 2018 prise à l'encontre de la société TEEMO et délibération n° 2018-287 du 5 juillet 2018 décidant de la rendre publique ;

◆ Mise en demeure n° 2018-023 du 25 juin 2018 prise à l'encontre de la société FIDZUP et délibération n° 2018-288 du 5 juillet 2018 décidant de la rendre publique ;

◆ Mise en demeure n° 2018-043 du 8 octobre 2018 prise à l'encontre de la société SINGLESPOT et délibération n° 2018-344 du 18 octobre 2018 décidant de la rendre publique ;

◆ Mise en demeure n° 2018-042 du 30 octobre 2018 prise à l'encontre de la société VECTAURY et délibération n° 2018-343 du 8 novembre 2018 décidant de la rendre publique.

Dans ces quatre dossiers, la société s'appuie sur une **technologie dénommée SDK**, afin de collecter des données à caractère personnel *via* les smartphones et d'effectuer des campagnes publicitaires mobiles auprès des personnes. Elle reçoit également des offres d'enchères en temps réel pour de l'espace publicitaire provenant d'applications tierces, avec lesquelles elle n'a aucun lien commercial.

À l'occasion de ses investigations, la CNIL a notamment constaté que **la société collecte des données de géolocalisation à travers son SDK**. La société conserve également, en vue de traitements ultérieurs, des données de géolocalisation contenues dans les enchères publicitaires, qu'elle reçoit d'applications ayant ou non installé son SDK. **Dans ces deux cas, la CNIL estime que le consentement des personnes n'est pas valablement recueilli**, et que de tels traitements constituent un **risque particulier au regard de la vie privée en ce qu'ils sont révélateurs des déplacements des personnes et de leurs habitudes de vie**.

La CNIL estime que la publicité de ces mises en demeure se justifie également par le **nombre massif de personnes susceptibles d'être impactées** par le traitement mis en œuvre par ces quatre sociétés, compte tenu du fait qu'une partie importante de la population est en possession d'un smartphone.
En effet, **le SDK est intégré à une vingtaine d'applications mobiles** et permet la collecte des données de **géolocalisation** des personnes environ **toutes les cinq minutes**.
La CNIL estime par ailleurs que la publicité des mises en demeure se fonde sur la **nécessité de mettre les personnes concernées en mesure de garder le contrôle de leurs données**. Cet objectif ne saurait être atteint qu'en assurant le plus haut niveau de transparence sur la collecte des données, notamment de géolocalisation, et la finalité du traitement mis en œuvre par ces quatre sociétés. La technicité de ces systèmes, et notamment les enchères publicitaires, rend ces **traitements largement inconnus du grand public**.

Enfin, la CNIL souhaite **sensibiliser les professionnels du secteur sur cette difficulté**, alors que la collecte de données à caractère personnel à des fins de profilage et de ciblage publicitaire, notamment à partir des lieux fréquentés par les personnes, connaît une forte

croissance. La CNIL note, en effet, que l'utilisation du SDK s'inscrit dans un écosystème faisant intervenir plusieurs acteurs, à savoir **les éditeurs d'applications mobiles et les clients annonceurs, qu'il est essentiel d'alerter** sur les enjeux de la protection des données.

Pour mémoire, il est rappelé que la mise en demeure ne revêt pas le caractère d'une sanction. À ce titre, aucune suite ne sera donnée à la procédure, si l'organisme concerné se conforme en tous points, aux exigences de la mise en demeure, dans le délai imparti. Si tel est le cas, celle-ci fera l'objet d'une clôture qui sera également rendue publique.

Mots Clé : CNIL – Mise en demeure – Technologie SDK – Géolocalisation des utilisateurs sans leur consentement – Utilisation des données de géolocalisation sans le consentement des utilisateurs – Risques importants d'atteintes à la vie privée des personnes – Applications mobiles – Smartphones – Technique de géolocalisation largement inconnue du grand public – Sensibilisation des professionnels du secteur : éditeurs d'applications mobiles et clients annonceurs – Sensibilisation du public

---

Pour d'autres articles d'actualité juridique, nous vous invitons à consulter notre site :

www.lexcontractus.fr

Vous pouvez librement vous abonner à notre newsletter (depuis la rubrique *Actualités juridiques* de notre site).
De même, vous pouvez librement vous en désabonner, par simple mail adressé à : cb@lexcontractus.fr

---

Mention légale :
Le présent bulletin est gratuit et ne peut être vendu.
Tous les droits de propriété intellectuelle (tels que notamment droits d'auteur, droits voisins, droits des marques) sont réservés. Ces éléments sont la propriété unique de la société d'exercice libéral à responsabilité limitée (SELARL) LEX CONTRACTUS, immatriculée au RCS de BORDEAUX sous le n° 519 133 219.
Toute utilisation non expressément autorisée entraîne une violation des droits d'auteur et constitue une contrefaçon. Elle peut aussi entraîner la violation de tous autres droits et réglementations en vigueur. Elle peut donc engager la responsabilité civile et/ou pénale de son auteur.
©LexContractus