LEGAVOX.fr
LA VOIX DU WEB JURIDIQUE

Condamnation d'un site internet par la CNIL pour ne pas avoir suffisamment protégé et conservé les données de ses utilisateurs

Jurisprudence publié le **19/08/2019**, vu **513 fois**, Auteur : Anthony Bem

La Commission nationale de l'informatique et des libertés peut-elle infliger une amende à un site internet pour ne pas avoir suffisamment protégé les données de ses utilisateurs et mis en œuvre les modalités de conservation de ces données ?

Les données à caractère personnel sur internet sont le pendant numérique de la vie privée.

L'exposition de données à caractère personnel sans contrôle d'accès préalable fait partie des vulnérabilités les plus répandues.

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.

Le cas échéant, la violation du droit au respect de la vie privée en ligne ou des données à caractère personnel peut être pécuniairement sanctionnée lourdement en France par la Commission nationale de l'informatique et des libertés (CNIL).

Ainsi, le 28 mai 2019, la CNIL a prononcé une sanction de 400.000 euros à l'encontre d'un site internet spécialisée dans la promotion immobilière, l'achat, la vente, la location et la gestion immobilière pour avoir insuffisamment protégé les données des utilisateurs de son site web et mis en œuvre les modalités de conservation des données (Délibération de la formation restreinte n° SAN – 2019-005 du 28 mai 2019 prononçant une sanction pécuniaire à l'encontre de la société SERGIC).

Pour cause, ce site permet notamment aux candidats à la location d'un bien immobilier de télécharger les pièces justificatives nécessaires à la constitution de leur dossier.

Or, un des utilisateurs du site a déposé une plainte auprès de la CNIL pour avoir pu accéder, depuis son espace personnel à des documents enregistrés par d'autres utilisateurs en modifiant légèrement l'adresse URL affichée dans le navigateur internet.

Un contrôle a permis de constater que près de 300.000 documents transmis par 30.000 candidats à la location étaient librement accessibles en ligne, sans authentification préalable.

Parmi ces documents figuraient des copies de cartes d'identité, de cartes Vitale, d'avis d'imposition sur le revenu, d'actes de décès, d'actes de mariage, d'attestations d'affiliation à la sécurité sociale, d'attestations délivrées par la caisse d'allocations familiales, d'attestations de pension d'invalidité, de jugements de divorce, de relevés de compte, de relevés d'identité bancaire et de quittances de loyers.

L'exploitation de la vulnérabilité ne requérait pas de maîtrise technique particulière en matière informatique.

En effet, la simple modification de la valeur de X dans l'adresse URL *https://www.crm.sergic.com/documents/upload/eresa/X.pdf* permettait à toute personne ayant connaissance de l'URL précitée de télécharger les documents en question, sans que la création préalable d'un compte sur le site soit nécessaire, et sans que cela requière une manipulation plus compliquée que la simple modification de la valeur X , qui correspond à un nombre.

La CNIL a ainsi considéré, d'une part, que le site internet avait manqué à son obligation de préserver la sécurité des données personnelles de ses utilisateurs et, d'autre part, qu'il conservait sans limitation de durée en base active l'ensemble des documents transmis par les candidats n'ayant pas accédé à la location au-delà de la durée nécessaire à l'attribution de logements.

En effet, selon le règlement général sur la protection des données (RGPD) 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, le responsable du traitement des données doit « *garantir un niveau de sécurité adapté au risque* ».

Il doit opter pour une série de techniques de protection comme la pseudonymisation et le chiffrement des données à caractère personnel, et « *des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement* ».

Ainsi, le responsable du traitement ou le sous-traitant évalue les risques inhérents au traitement et doit mettre en œuvre des mesures pour les atténuer, telles que le chiffrement afin de garantir la sécurité et de prévenir tout traitement effectué en violation du RGPD.

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.

La CNIL a ainsi jugé que le site internet avait manqué à son obligation d'assurer la sécurité des données personnelles traitées et n'avait pas mis en œuvre les moyens permettant de garantir leur confidentialité, afin d'empêcher qu'elles soient accessibles à des tiers non autorisés, conformément à l'article 32 du RGPD.

En effet, la CNIL a estimé que l'existence d'un défaut de sécurité sur le site a rendu possible la violation de données à caractère personnel dans la mesure où il a permis à des tiers non autorisés d'accéder à ces données.

En effet, lorsqu'une requête visant à accéder à une ressource est adressée à un serveur, celui-ci doit préalablement s'assurer que l'émetteur de cette requête est autorisé à accéder aux informations demandées.

En l'espèce, tout le monde pouvait librement consulter les documents transmis au site par un grand nombre de candidats à la location, sans qu'une mesure ne restreigne cette possibilité.

Cet accès aux documents conservés par le site traduisait une conception défectueuse du site, caractérisée en l'espèce par l'absence de mise en place d'une procédure d'authentification des utilisateurs.

La violation de données résultant de ce défaut de sécurité aurait pu être évitée si, par exemple, le site avait mis en œuvre un moyen d'authentification permettant de s'assurer que les personnes accédant aux documents étaient bien celles à l'origine de leur téléchargement sur le répertoire en question, et que seules celles-ci pouvaient y accéder.

La mise en place d'une telle fonctionnalité constitue une précaution d'usage essentielle, qui aurait permis de garantir la confidentialité des données personnelles traitées, conformément à l'article 32 du RGPD et de réduire significativement le risque de survenance de cette violation de données.

Au regard de ces éléments, la CNIL a considéré que le site n'avait 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 RGPD.

Surtout, la CNIL a estimé que le manquement à l'obligation de sécurité est aggravé au regard de la nature des données à caractère personnel rendues accessibles.

En effet, comme exposé précédemment, les documents transmis par les candidats à la location sont de nature très diverse et figuraient notamment, parmi les documents en question, des actes de mariage, des jugements de divorce, des contrats de travail, des documents relatifs à des prestations sociales ou encore des avis d'imposition.

Ces documents contiennent à la fois des données d'identification, telles que le nom, le prénom et les coordonnées, mais également une grande quantité d'informations susceptibles de révéler certains aspects parmi les plus intimes de la vie des personnes, comme les jugements de divorce.

Dans la mesure où le site traite des documents contenant des informations très précises sur certains aspects de la vie privée des personnes, la CNIL a considéré que la nécessité de mettre en place des mesures de sécurité proportionnées, permettant de garantir leur confidentialité, était d'autant plus importante.

Par ailleurs, s'agissant du manquement à l'obligation de conserver les données pour une durée proportionnée, l'article 5-1-e du RGPD dispose que :

« Les données à caractère personnel doivent être :

[…] e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ».

Or, le site conservait les documents transmis par les candidats n'ayant pas accédé à la location au-delà de la durée nécessaire à l'atteinte de la finalité pour laquelle les données personnelles ont été collectées et traitées - à savoir la location d'un bien immobilier - et ce sans que cette conservation ne soit encadrée par des garanties appropriées.

La durée de conservation des données personnelles doit être déterminée en fonction de la finalité poursuivie par le traitement.

Lorsque cette finalité est atteinte, les données doivent soit être supprimées, soit faire l'objet d'un archivage intermédiaire lorsque leur conservation est nécessaire pour le respect d'obligations légales ou à des fins précontentieuses ou contentieuses.

Ces données doivent alors être placées en archivage intermédiaire, pour une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont conservées.

Ainsi, après avoir opéré un tri des données pertinentes à archiver, le responsable de traitement doit prévoir, à cet effet, une base de données d'archives dédiée ou une séparation logique dans la base de données active.

Cette séparation logique est assurée par la mise en place de mesures techniques et organisationnelles garantissant que seules les personnes ayant un intérêt à traiter les données en raison de leurs fonctions, comme par exemple les personnes du service juridique, puissent y accéder.

Au-delà de ces durées de conservation des données versées en archives intermédiaires, les données personnelles doivent être supprimées.

En l'espèce, la collecte par le site de données personnelles des candidats a pour finalité l'attribution de logements.

Selon la CNIL, dès lors que cette finalité est atteinte, les données personnelles des candidats n'ayant pas accédé à la location ne pouvaient donc plus valablement être conservées au-delà de trois mois, au sein de la base de données active et au-delà faire l'objet d'une séparation logique voire d'un archivage intermédiaire.

Or, la CNIL a relevé que les documents transmis par les candidats n'ayant pas accédé à la location, c'est-à-dire ceux pour lesquels la poursuite du traitement n'était plus justifiée, n'étaient pas supprimés et qu'aucune purge n'était mise en œuvre en base de données.

Le site internet conservait en base active les données à caractère personnel des candidats n'ayant pas accédé à la location pour une durée excédant dans des proportions importantes celle nécessaire à la réalisation de la finalité du traitement, à savoir l'attribution de logements, sans qu'aucune solution d'archivage intermédiaire n'ait été mise en place.

Au regard de l'ensemble de ces éléments, la CNIL a considéré qu'un manquement à l'obligation de conservation des données, telle que prévue par l'article 5 du RGPD était caractérisé.

S'agissant des sanctions, il convient de garder en mémoire que le RGPD prévoit que lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du Règlement, il encourt une amende administrative ne pouvant excéder 20 millions d'euros ou, s'agissant d'une entreprise, 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

La CNIL veille aussi à ce que les amendes administratives soient *« effectives, proportionnées et dissuasives».*

Afin de décider du montant de l'amende administrative, la CNIL prend en compte notamment :

- 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 ;
- le fait que la violation a été commise délibérément ou par négligence ;
- toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées ;
- 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 ;
- toute violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant ;
- 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 ;
- les catégories de données à caractère personnel concernées par la violation;
- 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 ;

- 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.

En conséquence, la CNIL a décidé de prononcer à l'encontre du site internet une amende administrative d'un montant de 400.000 € et de rendre publique, sur son site et sur le site de Légifrance, sa décision qui sera anonymisée à l'expiration d'un délai de deux ans à compter de sa publication.

Je suis à votre disposition pour toute action ou information (en cliquant ici).

Anthony Bem
Avocat à la Cour
27 bd Malesherbes - 75008 Paris
Tel : 01 40 26 25 01

Email : abem@cabinetbem.com