A propos de la délibération de la CNIL à l'encontre de SERGIC

La CNIL prend ses précautions en sanctionnant l'agence immobilière SERGIC par une amende de 400 000 euros pour défaut de sécurité et non-respect des durées de conservation

Par Florent GASTAUD
Fondateur de Mon DPO externe

→RLDI 5583

Toute personne ayant déjà été confrontée à la recherche d'un bien immobilier en location aura pu constater que les documents demandés par les agences immobilières et/ou les propriétaires en amont de l'attribution de la location sont particulièrement nombreux et révélateurs de la vie privée du locataire et de son éventuelle caution.

Sur des marchés locatifs tendus, il n'est d'ailleurs pas rare pour un locataire de devoir déposer de nombreux « dossiers », aux fins d'espérer décrocher l'appartement de ses rêves. Et bien souvent, on peut légitimement se demander ce qu'il advient de ces quantités de données personnelles transmises.

La récente délibération de la Commission Nationale de l'Informatique et des Libertés (CNIL) à l'encontre de la société SERGIC[1], spécialisée dans l'achat, la vente, la location et la gestion immobilière, nous en donne un amer aperçu.

I.- À LA GENÈSE DE L'AFFAIRE : LA PLAINTE D'UN CITOYEN

A l'instar de nombreuses autres sanctions émanant de l'autorité française de protection des données personnelles, c'est la plainte d'un citoyen, utilisateur du site de la société SERGIC qui est à l'origine de cette affaire.

Constatant en mai 2018 un défaut de sécurité sur le site <www.sergic.com>, l'utilisateur a dans un premier temps le réflexe de prévenir l'éditeur du site. En l'absence de réponse et de mesures prises par ce dernier, l'internaute se tourne alors vers la CNIL en août de la même année.

Cette plainte va donner lieu au déclenchement de deux contrôles successifs de la part de la CNIL en septembre 2018 : dans un premier temps en ligne, puis au sein des locaux de la société SERGIC. Ces contrôles permettront de confirmer les éléments portés à l'attention de la CNIL par le plaignant et d'en découvrir de nouveaux. Deux griefs vont être reprochés à l'entité contrôlée : un manquement à ses obligations de sécurité des traitements de données personnelles mis en œuvre, ainsi qu'une conservation excessive des dites données.

Cette plainte a ainsi fait partie des 11 077 plaintes déposées auprès de la CNIL durant l'année 2018[2]. Elle va coûter cher à l'entité SERGIC et ne peut que rappeler toute l'importance de ce mécanisme.

II.- UN DÉFAUT DE SÉCURITÉ « CLASSIQUE » ET CONNU DU RESPONSABLE DE TRAITEMENT

A l'image de ce qu'avait pu constater le plaignant, la CNIL va établir qu'il était possible à tout individu, de consulter et de télécharger les pièces justificatives téléchargées par les presque 30 000 locataires ou potentiels locataires, ayant eu recours aux services de la société SERGIC.

Une fois le modèle d'URL connu – *qui était facilement connu par tout utilisateur du service* -, il suffisait de modifier un simple paramètre contenu au sein de ladite URL (en l'espèce, un nombre) pour accéder aux fameuses pièces justificatives. Au total, ce sont presque 300 000 documents qui étaient ainsi exposés.

Et pas n'importe quels documents ! La CNIL constate en effet la présence « *d'une grande quantité d'informations susceptibles de révéler certains aspects parmi les plus intimes de la vie des personnes* » dont des copies de cartes d'identité, de cartes Vitale, d'avis d'imposition, d'actes de décès ou de mariage, d'attestations

(1) Délibération de la formation restreinte n° SAN – 2019-005 du 28 mai 2019 prononçant une sanction pécuniaire à l'encontre de la société SERGIC : https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038552658&fastReqId=119744754&fastPos=1

(2) Rapport d'activité 2018 de la Commission Nationale de l'Informatique et des Libertés : https://www.cnil.fr/sites/default/files/atoms/files/cnil-39e_rapport_annuel_2018.pdf

d'affiliation à la sécurité sociale, etc. Des documents dont la compromission peut faire peser des risques particulièrement élevés pour les personnes concernées : risques d'usurpation d'identité, sentiment de violation de sa vie privée, etc.

Forte de ces constats, la CNIL reproche au spécialiste immobilier de ne pas avoir mis en œuvre les mesures techniques et organisationnelles appropriées afin de garantir la sécurité des données personnelles traitées sur son site, conformément aux exigences lui incombant en vertu des dispositions de l'article 32 et du considérant 83[3] du Règlement Général sur la Protection des Données (RGPD). Une obligation d'autant moins respectée que les mesures de sécurité déployées par SERGIC auraient dû être importantes, car proportionnées aux risques et à la nature des données à caractère personnel qu'elle se devait de protéger. Selon l'autorité française, « *La mise en œuvre d'une procédure d'authentification sur le site était une mesure élémentaire à prendre, qui aurait permis d'éviter la violation de données personnelles* ».

La CNIL est désormais habituée à constater ce type de défaillance de sécurité. Elle a en effet eu l'occasion de prononcer plusieurs sanctions pour des faits quasi-équivalents, notamment une sanction en janvier 2018 de 100 000€ à l'encontre de Darty[4], en mai 2018 de 250 000€[5] (ramenée à 200 000€ par le Conseil d'Etat[6]) à l'encontre d'Optical Center, de 250 000€ à l'encontre de Bouygues Telecom en décembre 2018[7].

III.- ABSENCE DE REMISE EN CAUSE DE LA PROPORTIONNALITÉ DES DONNÉES TRAITÉES

La proportionnalité et la légalité des données personnelles traitées par le spécialiste immobilier n'en sont pour autant pas contestées par la CNIL. En France, le décret n° 2015-1437 du 5 novembre 2015[8] vient fixer la liste des pièces justificatives pouvant être demandées au locataire et à sa caution (hors logements sociaux). L'objectif étant notamment d'évaluer la solvabilité des futurs locataires. Cette liste comporte de nombreux documents particulièrement sensibles et nous permet de mieux appréhender les documents étant concernés par les manquements du cas d'espèce :

- une pièce justificative d'identité en cours de validité (carte nationale d'identité, passeport, etc.) ;
- une seule pièce justificative de domicile (trois dernières quittances de loyer, attestation sur l'honneur de l'hébergeant indiquant que le candidat à la location réside à son domicile, dernier avis de taxe foncière, etc.) ;
- un ou plusieurs documents attestant des activités professionnelles du candidat locataire (contrat de travail, attestation de l'employeur, copie du certificat d'identification de l'INSEE pour un travailleur indépendant, etc.) ;
- un ou plusieurs documents attestant des ressources (avis d'imposition, trois derniers bulletins de salaires, etc.).

Fait intéressant, la société SERGIC se défend de ne pas avoir « *la maîtrise des pièces spontanément téléchargées par les candidats alors qu'elles ne figurent pas dans le décret précité* ». C'est d'ailleurs à ce titre que des copies de cartes vitales furent constatées comme faisant partie des données personnelles traitées par SERGIC, alors même qu'un tel document ne figure pas parmi de ceux pouvant être demandés aux futurs locataires pour prouver leur identité. Au sein de sa délibération, la CNIL ne semble pas en tenir rigueur à la société SERGIC en se contentant d'indiquer « *la formation restreinte ne remet pas en cause la nécessité pour la société SERGIC de disposer de la plupart de ces documents* ». Pourtant, le traitement de tels documents pourrait être considéré comme non-proportionné. Il aurait dès lors été intéressant de connaître la position de l'autorité à ce cas d'espèce et notamment si elle aurait pu exiger de la part de la société SERGIC la mise en place de mesures spécifiques pour éviter le traitement de « *pièces spontanées* » : une information renforcée particulièrement explicite à l'attention des locataires, une suppression manuelle des documents non-listés par le décret, etc. Il semblerait de toute évidence que la CNIL n'ait pas souhaité entrer dans de tels argumentaires.

IV.- NON-RESPECT DES DURÉES DE CONSERVATION

Second grief reproché par la CNIL à l'encontre de SERGIC : la conservation non proportionnée des données de locataires.

L'article 5-1-e) du RGPD impose en effet aux responsables de traitement de conserver toutes données personnelles pour « *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* (…) ».

A la lecture de la délibération de la CNIL, il est difficile de déterminer quelles étaient réellement les pratiques de la société SERGIC

(3) Articles 32 et considérant 83 du Règlement (UE) 2016/679 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 : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679

(4) Délibération de la formation restreinte n° SAN-2018-001 du 08/01/2018 prononçant une sanction pécuniaire à l'encontre de la société ETABLISSEMENTS DARTY ET FILS : https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000036403140&fastReqId=306045536&fastPos=1

(5) Délibération de la formation restreinte n° SAN-2018-002 du 7 mai 2018 prononçant une sanction pécuniaire à l'encontre de la société OPTICAL CENTER : https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000037013610

(6) C.E. 10ème - 9ème ch. réunies, 17 avr. 2019, 422575 : https://www.legifrance.gouv.fr/affichJuriAdmin.do?oldAction=rechJuriAdmin&idTexte=CETATEXT000038388015

(7) 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 : https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000037856073&fastReqId=2004200385&fastPos=1

(8) Décret n° 2015-1437 du 5 novembre 2015 fixant la liste des pièces justificatives pouvant être demandées au candidat à la location et à sa caution : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000031444493

en matière de durées de rétention. La société immobilière semble dans un premier temps, dans le cadre des contrôles menés par la CNIL, indiquer conserver sans limitation de durées les données personnelles traitées, avant de revoir sa position dans ses échanges écrits avec l'autorité française.

Seule certitude constatée par la CNIL lors de ses contrôles, SERGIC traitait des données datant de 2012 (soit environ depuis 6 ans) au sein de sa base de production active. Une durée justifiée pour le spécialiste immobilier car en adéquation avec le délai de prescription applicable à des faits de discrimination : 6 ans.

Conforme à sa doctrine[9], ainsi qu'à la lettre des dispositions du RGPD, la CNIL considère qu'une telle rétention de données est disproportionnée. SERGIC n'aurait pas dû traiter les données personnelles des candidats n'ayant pas accédé à la location plus de 3 mois au sein de sa base de production active. Une conservation ultérieure, qui n'était plus justifiée par la finalité du traitement, à savoir l'attribution des logements, aurait dû faire l'objet d'un archivage intermédiaire ou, *a minima*, d'une séparation logique. La CNIL rappelle en effet qu'il est parfaitement possible de conserver des données personnelles aux fins de respect d'obligations légales ou à des fins précontentieuses ou contentieuses, dès lors qu'une telle conservation fait l'objet d'un archivage intermédiaire.

V.- UNE SANCTION MESURÉE ET ARGUMENTÉE

La CNIL aura, sans le moindre doute, retenu quelques enseignements de l'arrêt du Conseil d'Etat d'avril 2019, ayant ramené la sanction prononcée à l'encontre d'Optical Center de 250k€ à 200k€[10]. L'autorité administrative indépendante se voyait reprocher de ne pas avoir suffisamment tenu « *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* » dans sa prise de décision.

Fort de cet enseignement, nous pouvons observer une plus grande rigueur dans les argumentaires déployés par la CNIL au sein de la délibération objet du présent article.

Le rapporteur désigné par la Présidente de la CNIL proposait, dans son rapport, le prononcé d'une sanction publique exorbitante de 900 000€ à l'encontre du spécialiste immobilier. La formation restreinte de l'autorité prononcera une sanction plus raisonnable de 400 000€ équivalente, tout de même, à environ 1% du chiffre d'affaire de l'entité SERGIC sur l'année précédant le prononcé de la sanction. Une somme déjà conséquente pour ce type d'acteur.

La CNIL justifie le montant de sa sanction au regard de différents éléments :

- le manque de célérité de la société dans la correction de la vulnérabilité, pendant une durée d'au moins six mois, qui aura eu pour effet de prolonger les risques sur les personnes concernées ;
- la nature des données personnelles concernées par le défaut de sécurisation ;
- le fait que les manquements constatés soient susceptibles de faire l'objet de sanctions pouvant aller jusqu'à 20M d'€ ou 4% du chiffre d'affaires annuel mondial.

Notons par ailleurs une défense relativement maladroite, sur certains aspects, de la part de la société SERGIC, ainsi qu'une absence de volonté de corriger une faille de sécurité - *connue en mai 2018 et seulement corrigée en septembre de la même année* -, au profit d'enjeux commerciaux : « *la société précise que ces délais s'expliquent par la forte demande de locations en période estivale et par la difficulté de suspendre ses activités durant cette période* ».

La formation restreinte de la CNIL aura davantage fait preuve de prudence dans sa présente délibération que par le passé. Elle aurait pu remettre en cause la proportionnalité des données traitées par la société SERGIC, mais ne s'y aventure pas. Elle aurait également pu reprocher à la société SERGIC de ne pas avoir notifié la violation de données personnelles[11] ayant été portée à sa connaissance dès mai 2018 par un internaute, mais ne s'y aventure pas, là non plus. ■

(9) Article publié sur le site de la CNIL, 28 mai 2018, « *Limiter la conservation des données* » : https://www.cnil.fr/fr/limiter-la-conservation-des-donnees

(10) C.E.10ème - 9ème ch. réunies, 17 avr.2019, n°422575 : https://www.legifrance.gouv.fr/affichJuriAdmin.do?oldAction=rechJuriAdmin&idTexte=CETATEXT000038388015

(11) Articles 33 et 34 du Règlement (UE) 2016/679 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 : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679