DONNÉES PERSONNELLES

L'obligation de sécurité : une obligation de moyen renforcée

La Cnil a prononcé une sanction de 400 000 € pour défaut de sécurité ayant permis une fuite de données et violation de l'obligation de conservation pour une durée limitée des données. Une augmentation significative du montant des condamnations prononcées par la Cnil sous l'empire du RGPD.

Le 25 mai 2018, le RGPD entrait en vigueur. Depuis lors, hormis la décision emblématique rendue à l'encontre de Google LLC à hauteur de 50 millions d'euros[1], peu de sanctions ont été prononcées par la Cnil sur le fondement du RGPD, car la plupart des décisions qui sont intervenues, bien que rendues postérieurement à cette entrée en vigueur, portaient sur des faits antérieurs.

La délibération de la formation restreinte de la Cnil du 28 mai 2019 qui sanctionne la société Sergic sur le fondement d'un manquement à la sécurité et à la confidentialité, au visa de l'article 32 du RGPD et sur le fondement du manquement à l'obligation de conservation pour une durée proportionnée, au visa de l'article 5 du RGPD, présente donc un intérêt particulier.

D'une part, elle permet de mesurer la portée de la nouvelle obligation instituée par l'article 32 du RGPD et de la comparer à l'obligation de sécurité qui pesait antérieurement sur les responsables de traitement, aux termes de l'article 34 de la loi du 6 janvier 1978 modifiée.
D'autre part, elle permet d'apprécier le montant d'une amende financière prononcée sous l'empire du RGPD et de le comparer à celui des sanctions prononcées sous l'empire de la loi antérieure pour le même type de manquement. L'on constate ainsi que la sanction infligée à Sergic à hauteur de 400 000 € représente le double, voire le triple, du montant des amendes prononcées sous l'empire de la loi antérieure par le régulateur français pour des manquements comparables.

Les faits

La société Sergic (ci-après Sergic) a une activité de gestion immobilière, dans le cadre de laquelle elle collecte, par le biais de son site, les pièces justificatives qu'elle demande aux candidats à la location d'un bien.

Le 12 août 2018, la Cnil est saisie d'une plainte d'un utilisateur qui indique que, par le biais d'une modification d'un caractère dans l'adresse URL du site, il a pu accéder aux pièces justificatives téléchargées par d'autres candidats à la location. Il indique en avoir informé Sergic dès mars 2018.

Le 7 septembre 2018, l'autorité procède à un contrôle en ligne. Sont alors téléchargés plus de 9 000 documents auxquels la délégation a pu accéder du fait de la faille de sécurité. Parmi ceux-ci se trouvent certaines données à caractère sensible ou encore à caractère hautement personnel, telles que des relevés d'identité bancaire ou des copies de cartes Vitale portant mention du NIR[2]. La délégation informe la société Sergic le jour même du défaut de sécurité.

Le 13 septembre 2018, la Cnil procède à un contrôle sur place et constate que le défaut de sécurité existe toujours. De plus, le responsable de traitement admet que les documents collectés

ne font l'objet d'aucune purge : les documents des candidats qui n'ont pas accédé à la location étant conservés en base active alors qu'ils ne sont pas réutilisés ultérieurement. Sergic reconnaît ainsi un manquement à l'obligation de conserver les données pour une durée proportionnée à la finalité du traitement.

Le rapporteur désigné propose à la formation restreinte de prononcer une sanction à hauteur de 900 000 €, ce qui représente environ 2% du chiffre d'affaire annuel de 43 millions d'euros. La formation restreinte prononcera finalement une amende administrative de 400 000 €, décidant de rendre la délibération publique, avec anonymisation de celle-ci à l'issue d'un délai de deux ans.

L'obligation de sécurité, une obligation de moyen renforcée ?

Le principal manquement sanctionné est le défaut de sécurité qui a permis la fuite de données.

Pour rappel l'article 32 du RGPD dispose que : « *compte tenu de la nature (...) du traitement ainsi que (...) des risques (...) pour les droits et libertés des personnes (...) le responsable de traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque (...).* »
Or, la formation restreinte rappelle qu'en l'espèce, le responsable de traitement n'avait pas mis en œuvre de procédure d'authentification des utilisateurs du site, ce qui traduit une conception défectueuse du site. Elle indique qu'il s'agit là d'une précaution d'usage essentielle qui aurait significativement réduit le risque de survenance de la violation de données. A cet égard, la Cnil rappelle que cette vulnérabilité est très répandue et que de nombreuses sanctions publiques ont déjà été prononcées pour des faits similaires.

Ainsi, à la question de savoir si l'article 32 du RGPD institue une obligation de sécurité qui serait renforcée par comparaison à celle qui était imposée antérieurement aux responsables de traitement aux termes de l'article 34 de la loi du 6 janvier 1978 modifiée[3], la décision ne permet pas d'apporter directement de réponse puisqu'en effet, l'autorité de contrôle souligne que le type de manquement commis par la société Sergic a été sanctionné maintes fois sous l'empire du droit antérieur au RGPD.

D'aucuns considèrent que si l'obligation de sécurité sous l'empire du droit antérieur[4] était interprétée comme posant une obligation de moyen, l'article 32 du RGPD poserait désormais une obligation de moyen renforcée. Ce débat porte principalement sur la charge de la preuve. Ainsi, en cas de survenance d'une faille de sécurité, si le responsable de traitement est tenu de rapporter la preuve, pour s'exonérer de sa responsabilité, de l'absence de tout manquement de sa part ou encore du fait d'un tiers, cela équivaut à lui imposer une obligation de résultat sur la sécurité. Si à l'inverse, le responsable de traitement peut se contenter de rapporter la preuve qu'il a mis en œuvre des mesures conformes à l'état de l'art pour prévenir le risque de fuite, comme c'était le cas sous l'empire du droit antérieur, il n'est tenu que d'une obligation de moyen.

Avec le RGPD, l'on peut considérer que le responsable de traitement est désormais tenu d'une obligation de moyen renforcée, notamment parce que celui-ci devient soumis au principe « *d'accountability* » qui l'oblige à établir la preuve de sa conformité au RGPD et, d'autre part, parce que le texte même de l'article 32 lui impose de mettre en œuvre des mesures appropriées au regard de la probabilité de survenance du risque et de l'atteinte qui pourrait en résulter aux droits et libertés des personnes.

En l'espèce, l'autorité de contrôle souligne que le manquement à l'obligation de sécurité est « *aggravé* » au regard du type de données rendues accessibles. Nous relevons à cet égard que la Cnil ne remet pas en cause le caractère proportionné de la collecte par rapport à la finalité du traitement, admettant l'argumentation de Sergic selon laquelle les pièces justificatives collectées étaient nécessaires à l'appréciation de la solvabilité des candidats et qu'ils correspondaient à une liste fixée par décret[5].

Toutefois si Sergic a pu collecter à bon droit ce type de données particulièrement identifiantes ou hautement personnelles, la Cnil considère que le manquement est aggravé du fait de l'absence de mesures de sécurité appropriées par rapport à la nature des données à protéger.

Cette délibération semble donc confirmer la position de la doctrine qui penche pour une obligation de sécurité de moyen renforcée.

Reste que Sergic a aussi péché par son manque de célérité à corriger la vulnérabilité dont elle avait été informée depuis mars 2018, laissant ainsi pendant six mois jusqu'en septembre 2018, les données accessibles. Sur ce point, l'argumentation de Sergic selon laquelle elle a fait le choix de privilégier la stabilité de son système d'information pendant l'été en raison de la forte demande de locations durant cette période, n'a guère été appréciée de l'autorité de contrôle.

Enfin, le fait d'avoir conservé en base active les documents transmis par les candidats n'ayant pas accédé à la location, alors même que la finalité du traitement était atteinte, est sanctionné sur le fondement de l'article 5 précité. La Cnil sanctionne Sergic pour avoir omis, soit de supprimer, soit de conserver ces données dans une base intermédiaire présentant des garanties appropriées.
C'est l'ensemble de ces éléments et circonstances aggravantes qui a amené l'autorité à fixer la sanction à 400 000 €.

Nous examinerons ci-après en quoi ce montant correspond à une augmentation significative du montant moyen de condamnation sous l'empire du RGPD et ce, dans la droite ligne de la tendance relevée auprès d'autres autorités de contrôle européennes.

Une augmentation significative du montant des sanctions prononcées sous l'empire du RGPD

La Cnil avait annoncé en juillet 2018, deux mois avant qu'elle reçoive la plainte de l'utilisateur qui l'a amenée à contrôler Sergic, qu'elle axerait ses contrôles pour l'année 2018 sur trois thématiques, «*choisies en raison du grand nombre de personnes concernées" et de «leur impact sur la vie quotidienne*» au nombre desquelles les pièces justificatives demandées par les agences immobilières aux candidats à la location. C'est donc sans doute avec à l'esprit l'exemple que l'autorité entendait faire de cette agence immobilière mais aussi plus généralement dans la perspective d'un renforcement général des condamnations avec l'avènement du RGPD que l'amende a été fixée.

A titre de comparaison, les délibérations rendues ces derniers mois par la Cnil sous l'empire du droit antérieur au RGPD, du fait de défaut de sécurité, ont abouti à des sanctions bien moindres.

Ainsi, le 19 juillet 2017, la société Hertz est condamnée à hauteur de 40 000 € après une fuite de données ayant permis d'accéder aux données personnelles de 40 000 clients[6]. Le 8 janvier 2018, la société Darty est condamnée à une amende administrative de 100 000 € à la suite d'une faille de sécurité ayant permis d'accéder aux données de 900 000 clients[7]. Enfin, le 7 mai 2018, la société Optical Center est condamnée à hauteur de 250 000 € du fait d'un défaut de sécurité sur son site qui rend accessibles les données de plus de 350 000 clients, y compris leur NIR et des données de santé, données sensibles[8]. En appel, le Conseil d'Etat9 ne ramène cette sanction à 200 000 € que du fait de la constatation de la célérité du responsable de traitement à apporter des mesures correctrices.

En revanche, la décision du CNPD (l'autorité de contrôle portugaise) rendue le 9 octobre 2018 sous l'empire du RGPD, à l'encontre de l'hôpital Barreiro[10], présente des similitudes notables avec la décision commentée. Ainsi, le régulateur portugais condamne le responsable de traitement à une amende de 400 000 €, notamment au visa des articles 5 et 32 du RGPD, pour violation de la confidentialité des données et du principe de minimisation des données. Il s'agit d'un niveau de sanction élevé, notamment motivé par l'accès donné à un personnel administratif n'ayant pas vocation à connaître les données médicales des patients.

Avec la décision Sergic, l'on assiste ainsi à la confirmation d'une tendance des autorités de contrôle à travers l'Union européenne à l'alourdissement des sanctions sous l'empire du RGPD. L'on constate toutefois que, jusqu'ici, le plafond de 2% ou 4% du chiffre d'affaires annuel est loin d'être atteint.

Il faudra attendre plusieurs décisions rendues sous l'empire du RGPD pour apprécier l'ampleur de la montée en puissance des attentes en matière de protection des données et des sanctions qui y sont associées.

Florence IVANIER
Avocat associé,
Cabinet Aurele IT
Data Protection Officer

Notes

(1) Délibération Cnil n° SAN 2019 001 du 21 janvier 2019

(2) Numéro d'Inscription au Répertoire (NIR) – numéro de sécurit sociale, donnée spécifiquement règlementée en France

(3) L'article 34 de loi de 1978 modifié par la loi du 6 août 2004 prévoit que « 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. »

(4) C'est-à-dire sous l'empire de la directive CE n° 95/46 du 24/10/1995 et plus particulièrement en France, sous l'empire de la loi du 6 janvier 1978 modifiée.

(5) décret du 5 novembre 2015 fixant la liste des pièces pouvant être demandées aux candidats à la location.

(6) Délibération Cnil n°SAN-2017-010

(7) Délibération Cnil n°SAN-2018-001

(8) Délibération Cnil n° SAN 2018-002

(9) Décision du Conseil d'Etat du 17 avril 2019

(10) Cette décision n'a pas été rendue publique en France mais on peut en lire des commentaires aux adresses URL suivantes

https://www.cio-online.com/actualites/lire-premiere-amende-rgpd-pour-un-hopital-portugais-10762.html

https://www.tripalio.fr/article/index/92b50bf835834454a2f9375fad200a68/rgpd-1ere-amende-nous-vient-portugal

https://mondelegueauxdonnees.fr/blog/la-cnil-portugaise-prononce-la-premiere-amende-en-application-du-rgpd/

Vous avez envie de vous exprimer sur un sujet qui vous tient à cœur, de partager votre analyse avec la communauté des lecteurs d'Expertises, d'exposer un point de vue différent sur un article déjà publié, de lancer un débat sur un thème émergent, ou simplement de commenter l'actualité du droit du numérique ?

Contactez la rédactrice en chef d'Expertises Sylvie Rozenfeld sr@expertises.info