N° 433311 – Société SERGIC

10ème et 9ème chambres réunies
Séance du 9 octobre 2020
Lecture du 4 novembre 2020

CONCLUSIONS

M. Alexandre Lallet, rapporteur public

La société requérante, spécialisée dans la gestion immobilière, offre aux candidats à la location d'un logement un service permettant de déposer sur son site internet les pièces justificatives nécessaires à leur dossier de candidature. En mars 2018, un utilisateur a constaté qu'il était possible de télécharger les documents personnels de personnes tierces moyennant une légère modification de l'adresse du site, ce qu'il a signalé à l'entreprise avant d'adresser une plainte à la CNIL en août. La CNIL a procédé le mois suivant à un contrôle à distance et sur place qui a confirmé cette faille de sécurité et révélé par ailleurs que SERGIC conservait les documents pendant une durée d'au moins six ans, alors même que les candidats à la location n'ont pas été retenus. Sur saisine de la présidente de la CNIL, la formation restreinte a prononcé en mai 2019 une amende de 400 000 euros, rendue publique sur son site Internet et sur Légifrance.

Les **infractions reprochées** ont commencé avant l'entrée en application du RGPD et l'entrée en vigueur de la loi n° 2018-493 du 20 juin 2018 qui a adapté le droit français au règlement européen, mais elles se sont poursuivies après. Dès lors que le droit antérieur qualifiait déjà de manquements les failles de sécurité et les durées de conservation excessives, il y a lieu, comme le juge la chambre criminelle en matière d'infraction pénale continue[1] et comme vous l'avez fait à plusieurs reprises, mais de manière inédite à notre connaissance[2], **d'appliquer pour le tout le régime répressif résultant de ces deux textes**.

Comme elle l'avait fait devant la formation restreinte, la société se plaint de ce que les agents de contrôle de la CNIL ont extrait des données depuis son site Internet dans le cadre du

[1] Cass. Crim. 11 févr. 1998, n° 96-84.997, au Bull.
[2] CE, 4 août 2006, *MINEFI c/ Sté Joseph Perasso*, n° 281946 ; CE, 5 novembre 2014, *Sté UBS France*, n° 371585.

contrôle à distance, en les téléchargeant, alors que le 3ème alinéa du III de l'article 44 de la loi du 6 janvier 1978 alors en vigueur leur permettait seulement de consulter et retranscrire les données.

Selon ce texte, les services de la CNIL peuvent procéder à toute constatation utile et « notamment », consulter les données librement accessibles ou rendues accessibles, y compris par négligence, et les retranscrire par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle. Il va de soi qu'une telle transcription peut consister à télécharger et envoyer par mail des documents ou à les fixer sur un support physique. Ces dispositions n'imposent certainement pas aux agents de recopier à la main des documents parfois nombreux, ni-même d'effectuer de fastidieux copier-coller ou des captures d'écrans. Le **téléchargement de données**, qui n'est rien d'autre qu'une copie électronique, s'assimile à la photocopie d'un document en cas de contrôle sur place. On ne trouve, dans les travaux préparatoires de la loi dite Hamon du 17 mars 2014 (n° 2014-344) qui a introduit ces dispositions, aucune trace d'une exclusion de ce procédé, et au contraire une volonté forte de renforcer les prérogatives d'investigation de la Commission dans le cadre du contrôle sur internet. De son côté, la société ne peut sérieusement tirer argument de l'arrêt de la chambre criminelle de la Cour de cassation du 20 mai 2015 (n° 14-81336, au Bull.) qui qualifie de vol l'intrusion dans un site extranet et le téléchargement sauvage de données, ce qui est sans le moindre rapport avec les pouvoirs d'investigation reconnus par la loi à une autorité de contrôle.

Le deuxième moyen de légalité externe consiste à reprocher à la CNIL d'avoir prononcé la sanction **sans mise en demeure préalable**. La société ne peut utilement se prévaloir de la décision *Sté Optical Center* du 19 juin 2017 (n° 396050, aux T.), rendue sous l'empire de la loi du 6 janvier 1978 dans sa rédaction antérieure à la loi pour une République numérique et qui exigeait alors une mise en demeure préalable, ni de la décision homonyme du 17 avril 2019 (n° 422575, aux T.), dans laquelle vous avez admis que la formation restreinte de la CNIL sanctionne un responsable de traitement sans mise en demeure préalable lorsque le manquement n'est pas susceptible d'être régularisé, car la loi de 1978 le prévoyait alors expressément.

Il résulte des termes mêmes du III de l'article 45 de la loi du 6 janvier 1978 dans sa version applicable en l'espèce que **la présidente de la CNIL peut soit choisir de prononcer une mise en demeure, soit saisir directement la formation restreinte, soit les deux en parallèle**, sans que ce choix fasse l'objet d'un encadrement textuel. La sanction directe n'est donc plus réservée au cas des manquements non régularisables ; la seule gravité d'un manquement peut parfaitement la justifier, sous votre contrôle[3]. C'est ce qui ressort des

[3] Même si cette mise en demeure ne constitue pas elle-même une sanction, la possibilité de la prononcer doit être prise en compte pour apprécier la proportionnalité de la sanction et conduire à l'annuler lorsque son caractère

travaux préparatoires de la loi de 2018[4], en cohérence avec la sévérité répressive exigée par le RGPD et la possibilité offerte par les articles 58 et 83 de ce règlement d'accompagner ou non une sanction pécuniaire par d'autres mesures correctrices, notamment une injonction de mettre fin au manquement. Le Conseil constitutionnel a déclaré ces dispositions de la loi de 2018 conformes à la Constitution dans sa décision n° 2018-765 DC du 12 juin 2018, sans l'assortir d'une quelconque réserve d'interprétation. Le commentaire aux cahiers relève expressément cette possibilité de sanction sans mise en demeure préalable.

Pour votre part, vous avez déjà jugé qu'aucun principe général du droit n'impose à une autorité administrative indépendante de mettre en demeure l'auteur d'un manquement d'y mettre fin avant de le sanctionner (CE, 27 juillet 2012, *SAS France Quick*, n° 325371, aux T.). Dans ses conclusions sur cette affaire, Edouard Crépey explique que l'exigence d'une mise en demeure préalable, posée par le Conseil constitutionnel dans sa décision n° 88-248 DC du 17 janvier 1989 concernant le CSA et reprise par votre décision d'Assemblée du 11 mars 1994, *SA « La Cinq »* (au Rec.), ne se justifie qu'en contrepartie de la possibilité laissée au législateur de ne pas prédéfinir les manquements susceptibles de faire l'objet d'une sanction administrative, et de renvoyer à l'ensemble des obligations pesant sur les sujets de droit. La mise en demeure permet alors de préciser la portée des griefs. Rien de tel ici, en tout état de cause. Et le règlement intérieur de la CNIL que brandit la société ne dit pas autre chose.

Quant au moyen d'erreur de droit reprochant à la CNIL d'avoir écarté des débats toute discussion du bien-fondé des décisions de la présidente de la CNIL en amont de la saisine de la formation restreinte, nous peinons à le comprendre alors que la délibération attaquée prend soin de répondre à cette critique et qu'elle n'était de toute façon pas tenue de faire la démonstration de sa propre régularité.

S'agissant de la durée de conservation des données, la décision attaquée est suffisamment motivée. Elle rappelle que, dans sa norme simplifiée NS-021 du 18 décembre 2003, la Commission avait recommandé de limiter la durée de conservation de telles données en base active à trois mois et, au-delà de cette durée, de détruire les données ou de les archiver dans une base distincte ou d'opérer une séparation logique avec les données actives, de sorte qu'elles ne soient plus accessibles pour la gestion courante mais continuent à être détenues afin de permettre au responsable de traitement de répondre à des obligations légales ou à des fins contentieuses ou précontentieuses. Et s'inspirant directement de cette recommandation en l'espèce, la formation restreinte a estimé que la perspective d'une action en discrimination dans l'accès au logement, qui se prescrit par six ans, que faisait valoir la société, justifiait tout au plus le stockage des données dans une base distincte et sécurisée.

---

véniel justifiait que la CNIL procède tout au plus par voie de mise en demeure.

[4] V. le rapport n° 350 de Mme Joissains du 14 mars 2018

Nous n'y voyons aucune erreur de raisonnement ni d'appréciation. La formation restreinte n'a nullement conféré à la norme simplifiée un caractère réglementaire qui l'aurait conduite à exclure par principe une conservation d'une durée supérieure à trois mois, pourvu qu'elle soit dûment justifiée. On peut gloser à l'infini du bien-fondé de cette durée de référence de trois mois, plutôt que quatre ou, comme le fait la société, cinq mois, en faisant valoir que la période de recherche de logements étudiants s'étale de mai à octobre. Ce qui est certain, c'est que la durée de six ans excède « *dans des proportions importantes* » celle nécessaire à la réalisation de la finalité pour laquelle les données sont collectées, à savoir l'attribution d'un logement. Vous observerez de surcroît que cette durée n'a pas été portée à la connaissance de la CNIL lors du contrôle et qu'aucun document n'atteste qu'elle avait réellement été fixée à l'époque, ce qui donne le sentiment qu'en réalité, la durée de conservation n'était pas limitée.

La société se plaint enfin du caractère disproportionné de la sanction. Indéniablement, l'amende infligée est particulièrement lourde puisqu'elle représente près de 1 % du chiffre d'affaires 2017 et près d'un quart du bénéfice net de la même année. Mais les deux manquements constatés sont à la fois flagrants et graves :

- s'agissant tout d'abord de la faille de sécurité, grief qui ne fait l'objet d'aucune contestation de fond, elle permettait d'accéder facilement à près de 300 000 fichiers concernant près de 30 000 personnes, dont des documents aussi sensibles que des contrats de travail, bulletins de salaires, avis d'imposition et justificatifs d'identité, comme des copies d'attestations de carte vitale faisant état du numéro de sécurité sociale (NIR). Ce manquement aurait pu être prévenu par une procédure d'authentification basique qui n'a pas été mise en place au moment de la conception du site. De surcroît, la société n'a manifestement pas pris la mesure de la gravité de la situation puisqu'il lui a fallu six mois pour y remédier, alors qu'il ne s'agit pas d'une PME récente, mais d'une société de taille respectable créée il y a plus de 50 ans.

- quant à la durée de conservation, déjà évoquée, elle est grossièrement excessive et d'autant plus regrettable que, comme on l'a vu, les documents stockés présentent une certaine sensibilité.

Pris isolément, le premier manquement pouvait justifier une sanction maximale de 10 millions d'euros en vertu du paragraphe 4 de l'article 83 du RGPD, le second, 20 millions d'euros. Conformément au paragraphe 3 du même article, c'est ce second plafond, le plus élevé, qui doit être retenu, s'agissant d'infractions multiples concernant un même traitement. L'écart à ce plafond s'explique par l'absence « d'antécédent judiciaire » de la société et l'absence de dommage avéré pour l'une des personnes concernées. La CNIL a d'ailleurs été sensible aux arguments de la société puisque le rapporteur proposait quant à lui un montant de 900 000 euros.

Sans doute le montant de 400 000 euros traduit-il un durcissement de la répression. Mais il est conforme au signal envoyé par le RGPD et opportun pour garantir la crédibilité des règles protégeant les données personnelles. Et nous ne sommes pas du tout convaincu qu'il soit incohérent avec les sanctions que brandit la société pour vous convaincre de réformer la sienne.

La plupart d'entre elles portent sur des **faits antérieurs à l'entrée en application du RGPD et qui étaient moins graves**, car n'incluant aucun grief sur la durée de conservation - qui est un manquement plus durement sanctionné par le RGPD - et concernant des sociétés qui avaient elles-mêmes signalé la faille de sécurité ou fait preuve d'une plus grande réactivité pour y remédier. Tel est le cas de la Société Optical Center, dont vous avez réduit l'amende de 250 000 à 200 000 euros pour une faille permettant d'accéder à des factures comportant notamment le NIR et la correction ophtalmologique des intéressés, afin de tenir compte de ses diligences dans la régularisation. Il en va de même d'Uber France[5] et de Bouygues Télécom[6], et même, sous l'empire du RGPD cette fois, d'Active assurances[7], société dont le chiffre d'affaires représentait environ le quart de celui de SERGIC, de sorte que l'amende de 180 000 euros infligée représentait une part plus importante de son chiffre d'affaires (1,8 % environ).

Dans ses dernières observations, la société requérante se prévaut, de manière plus pertinente, de la sanction infligée à SPARTOO, sous l'empire du RGPD. Cette entreprise de e-commerce s'est vu infliger une amende de 250 000 euros, soit seulement 0,2 % de son chiffre d'affaires groupe, pour quatre manquements, dont l'absence de durée de conservation et de purge des données des clients et des prospects, portant sur plusieurs millions de personnes, et la conservation non sécurisée des numéros de cartes bancaires utilisées par les clients. L'amende infligée correspond à environ 0,2 % du chiffre d'affaires connu du groupe.

On peut toutefois relever trois différences principales entre les deux affaires :

- d'une part, la très faible réactivité, pour ne pas dire l'indifférence initiale, de la société SERGIC. L'existence d'une faille de sécurité majeure aurait dû donner lieu à une notification spontanée à la CNIL, et, à tout le moins, au traitement diligent du signalement adressé par un utilisateur, qu'elle a largement ignoré. Elle continue d'ailleurs à se réfugier dans le déni voire la mauvaise foi – elle vous indique par exemple que, si la CNIL s'était adressée à ses services juridiques pendant le contrôle, elle aurait eu connaissance de la durée de conservation pratiquée…

[5] Délibération n°2018-011 du 19 décembre 2018
[6] Délibération SAN-2018-012 du 26 décembre 2018
[7] Délibération SAN 2019-007 du 18 juillet 2019

- d'autre part, la sensibilité particulière des données conservées et la diversité de ses informations portant sur une même personne, ouvrant la voie à des tentatives d'usurpation d'identité ;

- enfin, la situation financière de la SERGIC, entreprise bien installée et largement bénéficiaire, alors que SPARTOO, en phase de développement, était déficitaire.

Et au fond, s'il fallait critiquer une sanction, ce serait plutôt celle infligée à SPARTOO, qui nous paraît relativement clémente.

Nous vous proposons donc, sans état d'âme, de **confirmer la sanction pécuniaire**.

Quant à la publication nominative de la sanction, elle est cohérente avec la réputation de la SERGIC et justifié par la nécessité d'envoyer un signal clair aux bailleurs, et plus généralement aux entreprises auxquelles une faille de sécurité est signalée par un internaute. La motivation de la sanction est d'ailleurs mesurée dès lors qu'elle précise qu'il a été mis fin au premier manquement, que le second est en passe d'être résolu par le déploiement d'une solution technique d'archivage intermédiaire et que l'amende infligée est très inférieure à la proposition du rapporteur.

PCMNC au rejet de la requête.