REPUBLIQUE FRANCAISE
AU NOM DU PEUPLE FRANCAIS

Conseil d'État
10ème - 9ème chambres réunies
17 AVRIL 2019

N° 422575

M. Jacques Reiller, rapporteur
Mme Aurélie Bretonneau, rapporteur public
SCP GADIOU, CHEVALLIER, avocats

Vu la procédure suivante :

Par une requête et un mémoire en réplique enregistrés les 25 juillet 2018 et 1er avril 2019 au secrétariat du contentieux du Conseil d'Etat, la société Optical Center demande au Conseil d'Etat :

1°) d'annuler la délibération n° 2018-002 du 7 mai 2018 par laquelle la formation restreinte de la Commission nationale de l'informatique et des libertés (CNIL) a prononcé à son encontre une sanction pécuniaire d'un montant de 250 000 euros et décidé de rendre publique sa délibération pendant une durée de 2 ans à compter de sa publication ;

2°) à titre subsidiaire, de réduire significativement le montant de la sanction pécuniaire ;

3°) d'enjoindre à la CNIL de prononcer la clôture de la procédure, de préciser qu'elle a pu constater le 9 août 2017 que le site litigieux était en conformité, d'indiquer que sa décision du 7 mai 2018 a été prononcée sur des faits antérieurs à l'entrée en vigueur du "RGPD" et de publier ces éléments dans les mêmes conditions de publication que sa décision initiale ;

4°) de mettre à la charge de la CNIL la somme de 6 000 euros au titre de l'article L. 761-1 du code de justice administrative.

Vu les autres pièces du dossier ;

Vu :

- la loi n° 78-17 du 6 janvier 1978 ;
- la loi n° 2016-1321 du 7 octobre 2016 ;
- le code de justice administrative ;

Après avoir entendu en séance publique :

- le rapport de M. Jacques Reiller, conseiller d'Etat,

- les conclusions de Mme Aurélie Bretonneau, rapporteur public ;

La parole ayant été donnée, avant et après les conclusions, à la SCP Gadiou, Chevallier, avocat de la société Optical Center ;

Vu la note en délibéré, enregistrée le 3 avril 2019, présentée par la CNIL ;

Considérant ce qui suit :

1. Il résulte de l'instruction qu'un signalement a été reçu le 28 juillet 2017 par la Commission nationale de l'informatique et des libertés (CNIL), faisant état de données à caractère personnel qui auraient été rendues librement accessibles sur le site de la société Optical Center à partir de plusieurs " URL " ayant une structure identique. Le 31 juillet 2017, en application de la décision n° 2017-189 C de sa présidente, une délégation de la CNIL a effectué des vérifications en ligne 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 en effet 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. Après désignation par la présidente de la CNIL d'un rapporteur aux fins d'instruction et engagement de la procédure contradictoire, en vue d'une réunion de la formation restreinte qui s'est tenue le 22 février 2018, cette formation a décidé, par la délibération contestée du 7 mai 2018, de prononcer à l'encontre de la société Optical Center une sanction pécuniaire d'un montant de 250 000 euros et de rendre sa décision publique pendant une durée de 2 ans à compter de sa publication.

2. En premier lieu, le I de l'article 45 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, dispose que : " I. - Lorsque le responsable d'un traitement ne respecte pas les obligations découlant de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut le mettre en demeure de faire cesser le manquement constaté dans un délai qu'il fixe. En cas d'extrême urgence, ce délai peut être ramené à vingt-quatre heures. / Si le responsable du traitement se conforme à la mise en demeure qui lui est adressée, le président de la commission prononce la clôture de la procédure. / Dans le cas contraire, la formation restreinte de la commission peut prononcer, après une procédure contradictoire, les sanctions suivantes : 1° Un avertissement ; 2° Une sanction pécuniaire, dans les conditions prévues à l'article 47, à l'exception des cas où le traitement est mis en oeuvre par l'Etat ; 3° Une injonction de cesser le traitement, lorsque celui-ci relève de l'article 22, ou un retrait de l'autorisation accordée en application de l'article 25. / Lorsque le manquement constaté ne peut faire l'objet d'une mise en conformité dans le cadre d'une mise en demeure, la formation restreinte peut prononcer, sans mise en demeure préalable et après une procédure contradictoire, les sanctions prévues au présent I. ". Il résulte de ces dispositions, éclairées par les travaux préparatoires de la loi du 7 octobre 2016, 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.

3. Il résulte de l'instruction qu'à la suite d'une mesure correctrice apportée au traitement litigieux 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 s'ensuit que la formation restreinte de la CNIL a pu légalement, sur le fondement des dispositions citées au point précédent, engager, sans procéder à une mise en demeure préalable, une procédure de sanction à l'encontre de la société Optical Center.

4. En deuxième lieu, l'article 34 de la loi du 6 janvier 1978 dispose 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 ".

5. D'une part, 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. D'autre part, il ne résulte pas de l'instruction, en particulier de la production par courrier du 5 mars 2018, d'une pièce intitulée " Programme de protection " Bannir les activités anormales sur le site " " , que la société 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. Dans ces conditions, 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 précité.

6. En troisième lieu, l'article 47 de la loi du 6 janvier 1978 dispose: " Le montant de la sanction pécuniaire prévue au I de l'article 45 est proportionné à la gravité du manquement commis et aux avantages tirés de ce manquement. La formation restreinte de la Commission nationale de l'informatique et des libertés prend notamment en compte le caractère intentionnel ou de négligence du manquement, les mesures prises par le responsable du traitement pour atténuer les dommages subis par les personnes concernées, le degré de coopération avec la commission afin de remédier au manquement et d'atténuer ses effets négatifs éventuels, les catégories de données à caractère personnel concernées et la manière dont le manquement a été porté à la connaissance de la commission. / Le montant de la sanction ne peut excéder 3 millions d'euros. ".

7. 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. 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. Il sera fait une juste appréciation des circonstances de l'espèce en ramenant cette sanction pécuniaire à un montant de 200 000 euros.

8. Les motifs de la présente décision n'impliquent pas qu'il soit enjoint à la CNIL d'accomplir d'autres diligences. Au demeurant, la mention du constat par la CNIL de la mise en conformité du site litigieux est portée sur le site Légifrance et sur le site de la CNIL avec la publication de la décision attaquée. Toutefois, la présente décision, qui réforme la sanction pécuniaire infligée à la société Optical Center, implique que la CNIL en fasse une même publication.

9. Il n'y a pas lieu, dans les circonstances de l'espèce, de faire droit aux conclusions présentées par la société Optical Center au titre de l'article L. 761-1 du code de justice administrative.

D E C I D E :

Article 1er : La sanction pécuniaire de 250 000 euros infligée à la société Optical Center est ramenée à 200 000 euros.

Article 2 : La délibération de la formation restreinte de la Commission nationale de l'informatique et des libertés du 7 mai 2018 est réformée en ce qu'elle a de contraire à la présente décision.

Article 3 : Il est enjoint à la Commission nationale de l'informatique et des libertés de publier la présente décision.

Article 4 : Le surplus des conclusions de la requête est rejeté.

Article 5 : La présente décision sera notifiée à la société Optical Center et à la Commission nationale de l'informatique et des libertés.