CONSEIL D'ÉTAT - 10E ET 9E CHAMBRES RÉUNIES - 17 AVRIL 2019 - N° 422575

MOTS CLEFS : Données personnelles – CNIL – sanction pécuniaire – responsable de traitement

Par une délibération du 7 mai 2018, la CNIL avait infligé une amende de 250 000 € à la société Optical Center en raison d'une absence de sécurisation des données personnelles de ses clients. La société Optical Center faisant par de sa bonne foi refuse la décision et la porte devant le Conseil d'Etat, mais malheureusement ce dernier confirme la sanction de la CNIL.

FAITS : La CNIL avait constaté que les factures des clients e-commerce d'Optical Center étaient accessibles à tous sur internet en tapant une URL spécifique dans la barre d'adresse, et ce sans qu'il soit nécessaire de se connecter ou de s'authentifier. Ces factures comportaient notamment des noms, prénoms, adresses postales, corrections ophtalmologiques, dates de naissance, et numéros d'inscription au répertoire national d'identification des personnes physiques (numéros de sécurité sociale). Par ailleurs, la délégation de la CNIL 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.

PROCÉDURE : Lors d'un contrôle sur place effectué le 9 août 2017, la délégation de la CNIL a pu constater 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.

PROBLÈME DE DROIT : La formation restreinte de la CNIL et sans mise en demeure préalable, peut-elle 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 ?

SOLUTION : Le Conseil d'Etat a pris position identique à la CNIL confirmant la possibilité d'une sanction sans mise en demeure préalable pour manquement aux obligations de sécurisation des donnés de la part du responsable de traitement. C'est seulement sur l'appréciation du montant de la sanction que l'avis des deux entités diverge, le Conseil d'Etat retenant une amende d'un montant de 200 000€.

NOTE :

I. Confirmation de la sanction pour manquement aux obligations de sécurité sans mise en demeure préalable

Tout d'abord, avant de s'engager dans une analyse plus approfondie des faits d'espèce, le Conseil d'Etat rappelle la législation en vigueur applicable aux faits litigieux. En effet, la Haute Autorité considère qu'en raison de la temporalité des faits (juillet 2017), le litige doit être réglé selon la nouvelle rédaction de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, nouvelle dans sa rédaction depuis l'adoption de la loi du 7 octobre 2016 « Pour une République Numérique ». L'article 45 de ladite loi modifiée énonce que : *« 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 (…) 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. »*

Le Conseil d'Etat interprétant cet article à la lumière des travaux préparatoire de la loi du 7 novembre 2016 retient 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. »* On voit ici l'intérêt pour le Conseil d'Etat d'avoir rappelé le texte applicable, car en retenant comme applicable la loi du 6 janvier 1978 relative relative à l'informatique, aux fichiers et aux libertés dans sa nouvelle rédaction issue de la loi du 7 octobre 2016, cela lui permet d'interpréter les faits selon les travaux préparatoire de la loi modificatrice. On constate donc que le Conseil d'Etat est venu asseoir la légalité d'une sanction pécuniaire sur des travaux préparatoires, et non sur le texte de loi lui même. Toutefois, ceci n'est pas surprenant, puisque la loi du 7 octobre 2016 est le fruit de la transposition de la Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur. Or, il n'est pas rare de voir une instance de l'Union Européenne éclairer un litige à l'aide de travaux préparatoires, c'est même très fréquent. Par ailleurs en retenant une telle interprétation, le Conseil d'Etat agit surement dans l'idée d'être en accord avec le RGDP, qui justement clarifie ce point en son article 83.2 qui précise que les amendes administratives peuvent être imposées en complément ou à la place d'un avertissement, d'une injonction ou d'un rappel à l'ordre.

En outre, après le rappel du texte applicable, la Haute Autorité énonce les deux possibilités dans lesquelles une société peut être sanctionnée sans mise en demeure préalable. Le premier cas correspond à l'impossibilité de régularisation de la situation, et le second lorsqu'il a été remédié au manquement avant la décision de la CNIL. Pour le premier cas, le Conseil d'Etat ne reprend pas l'argument de la CNIL selon lequel un préjudice passé ne peut plus être régularisé (en mai 2018, la CNIL avait précisé qu'un incident de sécurité pouvait être réparé pour l'avenir mais non pour le passé), mais vise seulement les manquements « insusceptibles » d'être régularisés. Quant à lui, le second cas, a seulement pour intérêt d'inciter le responsable de traitement à mettre en oeuvre l'action préconisée par la CNIL. Si le responsable de traitement a déjà réalisé l'opération, la mise en demeure n'a plus d'objet. Pour le Conseil d'État, lorsque la mesure correctrice est apportée, la CNIL peut légalement engager une procédure de sanction, sans procéder à une mise en demeure préalable.

Par ailleurs, après confirmation de la validité de la sanction quant à l'absence de mise en demeure, le Conseil d'Etat confirme le manquement à l'obligation de sécuriser les données caractérisé par la société Optical Center :*« 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. »* Encore ici, le Conseil d'Etat reprend les arguments de la CNIL en caractérisant les manquements : *« 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 »* , mais aussi que *« 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 »*. Le Conseil d'État reproche également à la société Optical Center de ne pas avoir mis en place de protocole de tests en amont de la mise en production de son site internet ou de programme d'audits de sécurité ultérieurs.

Il rappelle enfin fermement 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 »*.

II. <u>Appréciation du pouvoir de sanction pécuniaire de la CNIL</u>

C'est seulement sur le montant de l'amende que le Conseil d'Etat va se voir plus indulgent que la CNIL. Tout d'abord rappelons que c'est l'article 45 de la loi du 6 janvier 1978 qui fixe (une longue) liste de critères à prendre en compte pour fixer l'amende. Pour le cas d'espèce, le Conseil d'Etat va faire une stricte application de cet article en appliquant méthodiquement chaque critère. Le Conseil d'État note tout d'abord que 334 769 documents étaient en libre accès, et qu'Optical Center n'a pas justifié avoir pris les précautions nécessaires à la sécurisation de son site web. Le caractère intentionnel ou de négligence du manquement est également pris en considération, ainsi que le degré de coopération afin de remédier au manquement et d'atténuer ses effets négatifs éventuels. Il relève aussi que le manquement avait cessé lors de l'instruction du dossier. Il n'était plus susceptible de faire l'objet d'une régularisation.

Cependant, *« 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. »* Alertée le 28 juillet 2017, elle avait réagi dès le 2 août selon l'arrêt. En conséquence, le montant de la sanction est réduit à 200 000 € et la CNIL devra procéder à la publication de la décision de réformation. On soulignera que cette solution est transposable au cadre juridique actuel, l'article 83 du RGPD imposant la proportionnalité dans la fixation des amendes administratives. Ce texte précise notamment que pour évaluer la somme, l'autorité de contrôle devra tenir compte du *« degré de coopération établi (...) en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs »*.

ARRÊT :
CONSEIL D'ETAT - 10E ET 9E CHAMBRES RÉUNIES - 17 AVRIL 2019 - N°422575

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.

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. 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.