Conseil d'État, 10ème - 9ème chambres réunies, 22/07/2022, 449694

FAITS : Un signalement a eu lieu sur un site internet indiquant l'existence de serveurs informatiques d'imagerie médicale précisant l'identité des patients, en libre accès. La CNIL (Commission nationale de l'informatique et des libertés) confirme le caractère librement accessible de telles données par des serveurs localisés en France. Elle a notifié au chirurgien du contrôle en ligne qu'elle avait effectué, après l'avoir informé du caractère librement accessible des images médicales de ses patients à partir de l'adresse IP de son serveur. Il a répondu avoir pris les mesures nécessaires pour mettre fin à la violation constatée. La CNIL a prononcé à l'encontre du chirurgien une amende administrative de 3 000 € au visa des articles 32 et 33 du RGPD pour manquement aux exigences élémentaires en matière de sécurité informatique ainsi que pour manquement à l'obligation de notification à la CNIL en cas de violation des données à caractère personnel.

PROCÉDURE : Le chirurgien saisi le Conseil d'État, demande, d'une part, l'annulation de cette délibération et d'autre part, demande à mettre à la charge de la CNIL la somme de 3 500 euros au titre de l'article L. 761-1 du code de justice administrative.

PROBLÉME DE DROIT : D'une part, le libre accès sur internet d'images médicales précisant l'identité des patients est-il constitutif d'un manquement aux exigences élémentaires en matière de sécurité informatique ? D'autre part, le responsable d'un tel manquement peut-il se voir exonérer de son obligation de notification à la CNIL, si cette dernière l'a elle-même informé du libre accès aux données et a engagé son contrôle ?

SOLUTION : Les juges confirment la délibération de la CNIL en ce qu'elle sanctionne le manquement aux exigences élémentaires en matière de sécurité informatique du chirurgien. Un libre accès à ces données dites sensibles constitue une violation de l'article 32 du RGPD.
Si les juges confirment le manquement au devoir de sécurité, il en va autrement pour la sanction relative au manquement à l'obligation de notification. En effet, l'arrêt précise « que l'obligation de notifier à la CNIL une violation de données à caractère personnel susceptible de faire naître un risque pour les droits et libertés des personnes physiques ne s'impose pas au responsable du traitement dans le cas où la CNIL l'a elle-même informé de cette violation et a engagé son contrôle sur la base des informations portées à sa connaissance par ailleurs ». Ainsi, la sanction pécuniaire est réduite à la somme de 2500 euros, le responsable de traitement est exonéré de son obligation de notification.

NOTE :

Sur le manquement aux exigences élémentaires en matière de sécurité informatique.

C'est sur la base de ce manquement que la Haute juridiction confirme, en partie, la délibération de la CNIL. En l'espèce, une faille informatique a engendré la mise en ligne de plus de cinq mille trois cents images médicales, assorties des noms, prénoms et dates de naissance des patients ainsi que de la date de réalisation de l'examen et du nom des praticiens concernés. Le chirurgien avait permis l'ouverture des ports réseaux sans mettre en place un dispositif de chiffrement des données à caractère personnel ce qui « permettait à toute personne prenant possession de ses appareils ou s'introduisant de manière indue sur le réseau auquel ces appareils étaient raccordés de prendre connaissance de ces données ». Ces données, sont des données de santé. Elles sont considérées comme des données à caractère sensible qui font l'objet d'une protection. Le RGPD, en son article 32, impose notamment au responsable de traitement la mise en place de « moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ». En l'espèce, ces données étaient en libre accès, c'est pour quoi les juges ont considéré que de telles circonstances étaient constitutives d'un manquement aux exigences élémentaires en matière de sécurité informatique tel que l'avait constaté la CNIL. Ainsi, sur le fondement de l'article 32 du RGPD, une sanction pécuniaire sera justifiée.

Sur le manquement aux exigences de notification à la CNIL.

L'article 33 du RGPD impose au responsable de traitement de notifier la violation de données à caractère personnel susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, à la CNIL. Cette notification doit être réalisée dans les meilleurs délais et si possible, dans les 72 heures au plus tard après en avoir pris connaissance. Cela implique, pour le responsable de traitement, de tenir un registre des violations de données à caractère personnel.
Classiquement, c'est cette notification qui permettra à la CNIL de déterminer si le responsable de traitement a failli à ses obligations. La CNIL pourra exercer ses prérogatives en mettant en œuvre ses pouvoirs d'enquête.
Mais la CNIL peut être informée de manquements aux obligations de sécurité et de l'existence de violations de données à caractère personnel via d'autres sources, notamment par voie de presse. Or, en l'espèce, c'est à travers un signalement sur internet que la CNIL a eu connaissance des faits et a pu engager son contrôle. Cependant, elle estime tout de même que « le responsable de traitement doit, en toute circonstance, respecter l'exigence de notification prévue à l'article 33 du Règlement à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques ». Sur ce point, le Conseil d'État infirme la décision de la CNIL. En effet, il considère « que l'obligation de notifier (…) ne s'impose pas au responsable du traitement dans le cas où la CNIL l'a elle-même informé de cette violation et a engagé son contrôle sur la base des informations portées à sa connaissance par ailleurs ». Naturellement, si la CNIL informe le responsable de traitement de ses manquements, la notification n'a plus de sens, elle perd sa raison d'être. Des lors, le responsable de traitement sera exonéré de son devoir de notification, mais sanctionné au titre de son

manquement aux exigences élémentaires en matière de sécurité informatique.

ARRÊT :

Vu la procédure suivante :

Par une requête sommaire et un mémoire complémentaire, enregistrés les 15 février et 17 mai 2021 au secrétariat du contentieux du Conseil d'Etat, M. D... C... demande au Conseil d'Etat :

1°) d'annuler la délibération n° SAN-2020-014 du 7 décembre 2020 par laquelle la formation restreinte de la Commission nationale de l'informatique et des libertés (CNIL) a prononcé à son encontre une amende de 3 000 euros ;

2°) de mettre à la charge de la Commission nationale de l'informatique et des libertés la somme de 3 500 euros au titre de l'article L. 761-1 du code justice administrative. (…)

1. Il résulte de l'instruction qu'à la suite du signalement sur le site internet " 01net.com " de l'existence, dans différents pays, de serveurs informatiques d'imagerie médicale en libre accès, les services de la Commission nationale de l'informatique et des libertés (CNIL) ont procédé les 20 et 24 septembre 2019 à des contrôles en ligne qui ont confirmé le caractère librement accessible de telles données par des serveurs localisés en France. Après avoir obtenu l'identité et les coordonnées des adresses IP afférentes, la délégation de contrôle de la CNIL a, par un courrier électronique du 8 octobre 2019, notamment, notifié à M. C..., chirurgien orthopédiste, le contrôle en ligne qu'elle avait effectué, après l'avoir informé du caractère librement accessible des images médicales de ses patients à partir de l'adresse IP de son serveur. Par un courrier électronique du 9 octobre 2019, M. C... a répondu avoir pris les mesures nécessaires pour mettre fin à la violation constatée. La formation restreinte de la CNIL a, par une délibération en date du 3 décembre 2020, prononcé à l'encontre de M. C... une amende administrative de 3 000 euros au titre des manquements constatés aux articles 32 et 33 du règlement du 27 avril 2016. M. C... demande l'annulation de cette délibération.

2. En premier lieu, le 1 de l'article 32 du règlement 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 des données, dit RGPD, dispose que : " Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins : / a) la pseudonymisation et le chiffrement des données à caractère personnel ; / b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ; / c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ; / d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement ".

3. Il résulte de l'instruction que la faille de sécurité informatique qui a conduit à mettre en libre accès plus de cinq mille trois cents images médicales, assorties des nom, prénom et date de naissance des patients, de la date de réalisation de l'examen et du nom des praticiens concernés, est imputable à l'installation informatique de M. C..., qui a

admis avoir, d'une part, procédé à l'ouverture des ports réseaux de la " box Internet " utilisée à son domicile pour faire fonctionner son " VPN ", dont il avait paramétré lui-même la fonction serveur du logiciel d'imagerie " HOROS " sans recourir à un prestataire et, d'autre part, omis de mettre en place un dispositif de chiffrement des données à caractère personnel figurant sur son disque dur externe, ce qui permettait à toute personne prenant possession de ses appareils ou s'introduisant de manière indue sur le réseau auquel ces appareils étaient raccordés de prendre connaissance de ces données. En estimant, eu égard à la sensibilité particulière de ces données de nature médicale, qu'un manquement aux exigences élémentaires en matière de sécurité informatique qui incombe à tout responsable de traitement était constitué, la formation restreinte de la CNIL n'a pas fait une inexacte application des dispositions de l'article 32 du RGPD.

4. En deuxième lieu, en vertu du paragraphe 1 de l'article 33 du RGPD, " en cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques ". Aux termes du paragraphe 3 du même article : " La notification visée au paragraphe 1 doit, à tout le moins: / a) décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés; / b) communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues; / c) décrire les conséquences probables de la violation de données à caractère personnel; / d) décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives ". Il résulte de ces dispositions que l'obligation de notifier à la CNIL une violation de données à caractère personnel susceptible de faire naître un risque pour les droits et libertés des personnes physiques ne s'impose pas au responsable du traitement dans le cas où la CNIL l'a elle-même informé de cette violation et a engagé son contrôle sur la base des informations portées à sa connaissance par ailleurs.

5. Il résulte de l'instruction que, par un courrier électronique en date du 8 octobre 2019, la CNIL a informé M. C... du libre accès des images médicales de ses patients à partir de l'adresse IP de son serveur et de l'engagement en conséquence d'un contrôle en ligne par ses services. Il s'ensuit qu'en retenant à l'encontre de M. C... un manquement à l'obligation de notification de la violation des données personnelles imposée par l'article 33 du RGPD, alors qu'eu égard à l'information dont disposait déjà la CNIL et qui lui avait permis d'engager un contrôle, ce dernier n'entrait pas dans le champ de cette obligation, la CNIL a entaché sa délibération d'une erreur de droit.

6. En dernier lieu, en vertu du 7° du III de l'article 20 de la loi du 6 janvier 1978, pour prononcer une amende administrative à l'encontre d'un responsable de traitement qui ne respecte pas les obligations résultant du RGPD, la formation restreinte de la CNIL prend en compte les critères précisés à l'article 83 de ce règlement, qui prévoit que les amendes administratives imposées par les autorités de contrôle nationales doivent, dans chaque cas, être " effectives, proportionnées et dissuasives ". Pour fixer le montant de l'amende, doivent, notamment, être pris en considération : " a)

la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi ; / b) le fait que la violation a été commise délibérément ou par négligence ; / c) toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées ; / d) le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre en vertu des articles 25 et 32 ; / e) toute violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant ; / f) le degré de coopération établi avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs ; / g) les catégories de données à caractère personnel concernées par la violation ; / h) la manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure, le responsable du traitement ou le sous-traitant a notifié la violation ; / i) lorsque des mesures visées à l'article 58, paragraphe 2, ont été précédemment ordonnées à l'encontre du responsable du traitement ou du sous-traitant concerné pour le même objet, le respect de ces mesures (…)

7. Il résulte de l'instruction que, pour fixer à 3 000 euros le montant de l'amende administrative infligée à M. C..., la formation restreinte de la CNIL a retenu que si ce dernier avait fait preuve de coopération avec l'autorité de contrôle en vue de remédier à la violation, il avait failli à deux principes en matière de sécurité informatique, d'une part, en ne protégeant pas son réseau informatique interne par la limitation des flux réseau au strict nécessaire, et, d'autre part, en ne procédant pas au chiffrement des données médicales concernées, et ce d'autant les données laissées accessibles étaient des données de santé qui doivent bénéficier de mesures de sécurité renforcées. Elle a aussi retenu un manquement à l'obligation de notification de la violation des données imposée par l'article 33 du RGP. Il résulte de ce qui a été dit aux points 3 et 5 que seul le manquement à l'article 32 du RGPD est constitué. Par suite, il sera fait une juste appréciation des circonstances de l'espèce en ramenant la sanction pécuniaire infligée à M. C... à un montant de 2 500 euros. (…)

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

D E C I D E :

Article 1er : Le montant de la sanction pécuniaire infligée à M. C... est réduit à 2 500 euros.

Article 2 : La délibération de la formation restreinte de la Commission nationale de l'informatique et des libertés du 7 décembre 2020 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 sur son site internet et sur le site Légifrance sans identifier le responsable de traitement.

Article 4 : Le surplus des conclusions de la requête de M. C... est rejeté.
Article 5 : La présente décision sera notifiée à M. D... C... et à la Commission nationale de l'informatique et des libertés.