Délibération SAN-2019-014 du 7 décembre 2020

Commission Nationale de l'Informatique et des Libertés
Nature de la délibération : Sanction
Etat juridique : En vigueur
Date de publication sur Légifrance : Jeudi 17 décembre 2020

Délibération de la formation restreinte no SAN-2020-014 du 7 décembre 2020 concernant Monsieur [...]

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de Messieurs Alexandre LINDEN, président, Philippe-Pierre CABOURDIN, vice-président, et de Mesdames Dominique CASTERA, Anne DEBET et Christine MAUGÜE, membres ;

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 20 et suivants ;

Vu le décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision n° 2019-152C du 20 septembre 2019 de la présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification des traitements notamment accessibles à partir de l'adresse IP portant le numéro [...] ;

Vu la décision de la présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur devant la formation restreinte, en date du 27 juillet 2020 ;

Vu le rapport de Monsieur François PELLEGRINI, commissaire rapporteur, notifié à Monsieur [...] le 23 septembre 2020 ;

Vu les observations orales formulées lors de la séance de la formation restreinte ;

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte du 3 décembre 2020 :

- Monsieur François PELLEGRINI, commissaire, entendu en son rapport ;

En qualité de représentant de Monsieur [...] :

- [...] ;

Le conseil de Monsieur [...] ayant eu la parole en dernier ;

La formation restreinte a adopté la décision suivante :

I.Faits et procédure

1. M. [...] exerce une activité libérale [...] à Paris [...].
2. Le […], le site web […], a signalé l'accès libre à des serveurs informatiques d'imagerie médicale situés […] permettant la consultation et le téléchargement […] d'images médicales (IRM, radios, scanners, etc…) suivies notamment des nom, prénoms, date de naissance et date de consultation des patients.
3. En application de la décision n° 2019-152C du 20 septembre 2019 de la présidente de la Commission nationale de l'informatique et des libertés (ci-après la CNIL ou la Commission), les services de la CNIL ont procédé à un contrôle en ligne, les 20 et 24 septembre 2019, qui a confirmé le caractère librement accessible de ces données, exploitables par l'intermédiaire d'un simple logiciel de consultation d'images médicales. Le contrôle a également permis d'établir la liste des adresses IP de ces serveurs qui sont localisées en France.
4. Ce contrôle avait notamment pour objet de vérifier le respect, par les attributaires de ces adresses IP, de l'ensemble des dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après le

Règlement ou le RGPD) et de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (ci-après la loi informatique et libertés).

5. Après avoir demandé aux différents fournisseurs d'accès à Internet de leur communiquer l'identité et les coordonnées des responsables de traitement utilisant ces adresses IP françaises, les services de la CNIL ont été informés que l'une de ces adresses, portant le numéro [...], avait pour attributaire M. [...].
6. Par un courrier électronique du 8 octobre 2019, la délégation de contrôle a notifié le contrôle en ligne à M. [...], après l'avoir informé du caractère librement accessible des images médicales de ses patients à partir de l'adresse IP de son serveur.
7. Par un courrier électronique du 9 octobre, M. [...] a répondu avoir pris les mesures nécessaires pour mettre fin à la violation.
8. Le 6 décembre 2019, M. [...] a été auditionné par la délégation de contrôle dans les locaux de la CNIL. Il a indiqué que pour pouvoir accéder à distance aux images médicales hébergées dans le disque dur de l'ordinateur fixe de son domicile, il a *ouvert les ports de la LiveBox utilisée à son domicile en activant le mode DMZ de cette dernière, dans l'objectif de faire fonctionner le VPN* .
9. Aux fins d'instruction de ces éléments, la présidente de la Commission a désigné M. François PELLEGRINI en qualité de rapporteur, le 27 juillet 2020, sur le fondement de l'article 22 de la loi informatique et libertés .
10. À l'issue de son instruction, le rapporteur a fait remettre en main propre à M. [...], le 23 septembre 2020, un rapport détaillant les manquements au RGPD qu'il estimait constitués en l'espèce. Le même jour, les services de la CNIL lui ont notifié une convocation à la séance de la formation restreinte du 3 décembre 2020.
11. Ce rapport proposait à la formation restreinte de la Commission de prononcer une amende administrative à l'encontre de M. [...] au titre de manquements aux articles 32 et 33 du Règlement.
12. Le 20 novembre 2020, M. [...] a sollicité, par l'intermédiaire de son conseil, le report de la séance de la formation restreinte. Cette demande a été rejetée le 26 novembre 2020 par le président de la formation restreinte.
13. Le conseil de M. [...] et le rapporteur ont présenté des observations orales lors de la séance de la formation restreinte.

II.Motifs de la décision

A.Sur le manquement à l'obligation d'assurer la sécurité des données traitées

14. Aux termes de l'article 32, paragraphe 1, du RGPD, *le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque* .

15. Les a) et b) de ce même paragraphe 1 prévoient qu'en fonction notamment de *la portée, du contexte et des finalités du traitement ainsi que des risques* pour les personnes concernées, le responsable de traitement met en œuvre *le chiffrement des données à caractère personnel* et *des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement* .

16. Le rapporteur fait valoir que la vulnérabilité du dispositif d'imagerie médicale à l'origine de la violation de données est imputable à M. [...] qui n'a pas mis en œuvre les mesures techniques appropriées pour garantir la sécurité du traitement.

17. Le conseil de M. [...] répond que son client n'avait aucune volonté de laisser un libre accès à ces images médicales et que la violation n'est que la conséquence malheureuse du raccordement à sa box Internet du disque dur externe branché à l'ordinateur de son domicile.

18. La formation restreinte relève qu'en application de l'article 32 du RGPD, il incombait à M. [...], en tant que responsable de traitement, de veiller à la sécurité des données qu'il traitait dans le cadre de son activité professionnelle.

19. Tout d'abord, la formation restreinte souligne qu'il n'est pas contesté que la violation de données a pour cause l'ouverture des ports réseaux de la box Internet utilisée au domicile de M. [...] couplée au paramétrage de la fonction serveur du logiciel d'imagerie [...] .

20. Elle relève que dans son courrier électronique du 9 décembre 2019, M. [...] a indiqué : *il se trouve que ce logiciel [le logiciel d'imagerie [...]] comprend une fonction serveur, que le mac est derrière une LiveBox connectée à Internet et que (…) je pense que le port de 11112 de la LiveBox est ouvert à tous vents* . Par ailleurs, dans le cadre de son audition du 6 décembre 2019, ce dernier a précisé n'avoir *pas eu recours à un prestataire pour l'installation et le paramétrage du logiciel [...]* et avoir lui-même *ouvert les ports de la LiveBox utilisée à son domicile (…) dans l'objectif de faire fonctionner le VPN* .

21. Il ressort donc de ces éléments que M. [...] n'avait pas pris soin de limiter les fonctions réseaux à celles qui étaient strictement nécessaires au fonctionnement du traitement.

22. Or, la formation restreinte souligne que la protection du réseau informatique interne et le chiffrement des données à caractère personnel font partie des exigences élémentaires en matière de sécurité informatique, qui incombent à tout responsable de traitement.

23. A cet égard, dans le guide *La sécurité des données personnelles* , qui offre un éclairage utile aux responsables de traitement quant aux mesures à mettre en œuvre afin de garantir la sécurité de leur traitement, la Commission recommande d' *autoriser uniquement les fonctions réseau nécessaires aux traitements mis en place* . De même, le *Guide pratique pour les médecins* , publié par la CNIL en concertation avec le Conseil national de l'ordre des médecins, invite les médecins à limiter le plus possible la connexion d'appareils non professionnels sur le réseau au sein duquel sont traitées les données des patients, ainsi qu'à recourir à des moyens d'authentification forte pour accéder à ce réseau.

24. Ensuite, la formation restreinte souligne qu'il ressort également de l'audition du 6 décembre 2019 que M. [...] n'avait pas non plus pris soin de chiffrer les données contenues dans ses trois ordinateurs portables et dans son ordinateur fixe.

25. Or, en l'absence de chiffrement, les données médicales contenues dans le disque dur de ces ordinateurs étaient lisibles en clair par toute personne prenant possession de ces appareils (par exemple, à la suite de leur perte ou de leur vol) ou par toute personne s'introduisant de manière indue sur le réseau auquel ces appareils étaient raccordés.

26. A cet égard, dans son guide *La sécurité des données personnelles* , la CNIL recommande de prévoir des moyens de chiffrement des postes nomades et supports de stockage mobiles (ordinateur portable, clés USB, disque dur externes, CD-R, DVD-RW, etc.), par exemple *via* le chiffrement du disque dur dans sa totalité lorsque le système d'exploitation le propose, le chiffrement fichier par fichier ou la création de conteneurs (fichier susceptible de contenir plusieurs fichiers) chiffrés. De même, le Guide pratique pour les médecins invite les médecins à procéder au chiffrement des données de leurs patients avec un logiciel adapté.

27. Enfin, la formation restreinte relève que le traitement en cause concerne des données médicales, qui constituent des catégories particulières de données à caractère personnel, au sens de l'article 9 du Règlement. La nature de ces informations appelait donc une vigilance toute particulière afin d'éviter une violation de données.

28. La formation restreinte rappelle ainsi que parmi les données concernées par la violation, figuraient, outre les images médicales, les nom, prénoms et date de naissance du patient, la date de réalisation de l'examen, le nom du praticien référent et du praticien ayant réalisé l'examen et le nom de l'établissement dans lequel celui-ci avait eu lieu.

29. Elle souligne qu'il ressort des propres déclarations de M. [...] dans le cadre de son audition du 6 décembre 2019 que plus de cinq mille trois cents séries d'images médicales sont concernées.

30. Enfin, elle relève qu'il ressort du dossier que ces données ont été exposées environ quatre mois.

31. Au regard de l'ensemble de ces éléments, la formation restreinte considère qu'un manquement à l'article 32 du RGPD est constitué.

B.Sur le manquement à l'obligation de notifier la violation de données à la CNIL

32. Aux termes de l'article 33, paragraphe 1, 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 .*

33. Le rapporteur fait valoir que M. [...] n'a pas déclaré la violation de données auprès des services compétents de la Commission.

34. M. [...] répond que la nécessité de notifier la violation de données à la Commission ne lui a jamais été indiquée. Il invoque, par ailleurs, le caractère artificiel d'une telle obligation dès lors qu'il a eu connaissance du libre accès de son serveur d'imagerie médicale par la délégation de contrôle de la CNIL.

35. La formation restreinte considère que le responsable de traitement doit 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. La circonstance que la violation de données ait été portée à la connaissance de M. [...] par le service des contrôles de la CNIL ne le déchargeait pas de cette obligation.

36. En effet, consécutivement au contrôle, le responsable de traitement peut avoir connaissance d'éléments complémentaires relatifs à la violation de données qui méritent d'être communiqués aux services compétents de la CNIL, lesquels ont notamment pour mission de centraliser les différentes violations de données et d'en assurer le suivi afin de prévenir la compromission de données à caractère personnel. Un téléservice est disponible sur le site de la CNIL pour effectuer ces notifications.

37. En l'espèce, la formation restreinte rappelle que l'existence et la nature de l'obligation de notification figuraient dans le courrier électronique du 8 octobre 2019 qui informait M. [...] de ladite violation de données.

38. La formation restreinte considère donc qu'un manquement à l'article 33 du Règlement est constitué.

III.Sur les mesures correctrices et la publicité

39. Aux termes du III de l'article 20 de la loi informatique et libertés :

Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut également, le cas échéant après lui avoir adressé l'avertissement prévu au I du présent article ou, le cas échéant en complément d'une mise en demeure prévue au II, saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes : […]

7° À l'exception des cas où le traitement est mis en œuvre par l'État, une amende administrative ne pouvant excéder 10 millions d'euros ou, s'agissant d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Dans les hypothèses mentionnées aux 5 et 6 de l'article 83 du règlement (UE) 2016/679 du 27 avril 2016, ces plafonds sont portés, respectivement, à 20 millions d'euros et 4 % dudit chiffre d'affaires. La formation restreinte prend en compte, dans la détermination du montant de l'amende, les critères précisés au même article 83.

40. L'article 83 du RGPD prévoit :

1. Chaque autorité de contrôle veille à ce que les amendes administratives imposées en vertu du présent article pour des violations du présent règlement visées aux paragraphes 4, 5 et 6 soient, dans chaque cas, effectives, proportionnées et dissuasives.

2. Selon les caractéristiques propres à chaque cas, les amendes administratives sont imposées en complément ou à la place des mesures visées à l'article 58, paragraphe 2, points a) à h), et j). Pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative, il est dûment tenu compte, dans chaque cas d'espèce, des éléments suivants :

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 ;

j) l'application de codes de conduite approuvés en application de l'article 40 ou de mécanismes de certification approuvés en application de l'article 42 ; et

k) toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation.

41. Concernant le prononcé d'une amende administrative, le conseil de M. [...] estime notamment que la mesure correctrice proposée par le rapporteur est disproportionnée au regard de sa responsabilité dans la violation de données et que le prononcé d'un rappel à l'ordre serait plus justifié.

42. Il revendique également le fait d'avoir réagi très rapidement pour mettre un terme à la violation, dès qu'il en a eu connaissance par la délégation, et fait valoir sa pleine coopération avec les services de la Commission.

43. La formation restreinte rappelle que pour apprécier l'opportunité de prononcer une amende administrative il convient de se référer aux critères pertinents précisés par l'article 83, paragraphe 2, du RGPD.

44. En l'espèce, elle estime qu'il convient de faire d'abord application du critère prévu à l'alinéa f) de l'article 83, paragraphe 2, du Règlement relatif au degré de coopération établi avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs.

45. La formation restreinte relève que dès qu'il a eu connaissance de la violation, M. [...] a immédiatement pris les mesures nécessaires permettant d'y mettre un terme aussitôt.

46. Elle rappelle ainsi que dans son courrier électronique du 9 octobre 2019 en réponse à la délégation de contrôle, M. [...] a indiqué avoir *désactivé la fonction serveur du logiciel et bloqué les ports non utiles sur la Livebox* .

47. Cependant, la formation restreinte souligne qu'il convient de faire également application des critères prévus aux alinéas a) et g) de l'article 83, paragraphe 2, du Règlement relatifs, d'une part, à 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 d'autre part, aux catégories de données à caractère personnel concernées par la violation.

48. Elle relève ainsi que M. [...] a failli à deux principes élémentaires en matière de sécurité informatique, à savoir la protection du réseau informatique interne par la limitation des flux réseau au strict nécessaire et le chiffrement des données à caractère personnel.

49. La formation restreinte souligne à nouveau que la gravité du manquement à l'article 32 du RGPD est d'autant plus caractérisée que des données de santé sont concernées et que cette catégorie particulière de données à caractère personnel doit bénéficier de mesures de sécurité renforcées, conformément au considérant 75 du RGPD.

50. Elle répète que le non-respect de ces pratiques élémentaires a eu pour conséquence directe de rendre accessibles plus de cinq mille trois cents séries d'images de santé comprenant, pour chacune de ces séries, outre l'image médicale, les nom, prénoms et date de naissance de chaque patient, la date de réalisation de l'examen, le nom du praticien référent et du praticien ayant réalisé l'examen et le nom de l'établissement dans lequel celui-ci a eu lieu.

51. Elle rappelle que les données à caractère personnel hébergées sur le disque dur de l'ordinateur fixe du domicile de M. [...] sont restées accessibles sans aucune authentification pendant une durée d'environ quatre mois.

52. Enfin, la formation restreinte souligne qu'il convient également de faire application du critère prévu à l'alinéa h) de l'article 83, paragraphe 2 du Règlement relatif à la manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure, le responsable du traitement a notifié la violation.

53. Elle rappelle en l'occurrence que la Commission a eu connaissance de la violation de données par le biais d'un article de presse et que M. [...] ne l'a jamais notifiée aux services compétents de la Commission, même après que la délégation de contrôle a attiré son attention sur ce point.

54. Au regard de ces éléments, la formation restreinte considère nécessaire le prononcé d'une amende administrative à l'encontre de M. [...].

55. Concernant la détermination du montant de cette amende, la formation restreinte considère que le manquement à l'article 32 du RGPD présente une gravité certaine, qu'en revanche le manquement à l'article 33 présente en l'espèce un caractère formel.

56. Elle note que selon les déclarations de son conseil lors de la séance du 3 décembre 2020, M. [...] a perçu 97 000 € de revenus en 2018 et qu'en application des dispositions de l'article 83, paragraphe 4, du RGPD, il encourt une sanction financière d'un montant maximum de 10 millions d'euros.

57. Dès lors, au regard des capacités financières de M. [...] et des critères pertinents de l'article 83, paragraphe 2, du Règlement, la formation restreinte estime que le prononcé d'une amende de 3 000 € apparaît à la fois effectif, proportionné et dissuasif, conformément aux exigences de l'article 83, paragraphe 1, de ce Règlement.

PAR CES MOTIFS

La formation restreinte de la CNIL, après en avoir délibéré, décide de :

- **prononcer à l'encontre de M. [...] une amende administrative d'un montant de 3 000 € (trois mille euros) pour les manquements aux articles 32 et 33 du RGPD ;**
- **rendre publique cette décision sur le site de la CNIL et sur le site de Légifrance sans identifier le responsable de traitement.**

Le président

Alexandre LINDEN

Cette décision est susceptible de faire l'objet d'un recours devant le Conseil d'État dans un délai de deux mois à compter de sa notification.