CNIL, formation restreinte, délibération SAN-2026-009 du 21 juillet 2026

Source : https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000054790100

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de M. Philippe-Pierre CABOURDIN, président, M. Vincent LESCLOUS, vice-président, Mmes Laurence FRANCESCHINI et Isabelle LATOURNARIE-WILLEMS, MM. Didier KLING et Bertrand du MARAIS, membres, Vu le règlement (UE) 2016/679 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 de ces données ;

Vu la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 20 et suivants ;

Vu le code de la santé publique ;

Vu le décret no 2019-536 du 29 mai 2019 pris pour l'application de la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération no 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° 2025-1154 QPC du 8 août 2025 du Conseil constitutionnel ;

Vu la décision n° 2025-125C du 7 juillet 2025 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 mis en œuvre par la société HOPITAL PRIVE DE LA LOIRE ou pour son compte ;

Vu la décision de la présidente de la Commission nationale de l'informatique et des libertés du 19 février 2026 portant désignation d'une rapporteure devant la formation restreinte ;

Vu le rapport de Mme Anne DEBET, commissaire rapporteure, signifié à la société HOPITAL PRIVE DE LA LOIRE le 5 mars 2026 ;

Vu les observations écrites versées par la société HOPITAL PRIVE DE LA LOIRE le 3 avril 2026 ;

Vu la clôture de l'instruction, notifiée à la société le 18 mai 2026 ;

Vu le courrier du président de la formation restreinte du 18 mai 2026, informant la société que le dossier était inscrit à l'ordre du jour de la formation restreinte du 18 juin 2026 ;

Vu les observations orales formulées lors de la séance de la formation restreinte du 18 juin 2026 ;

Vu les autres pièces du dossier, Étaient présents, lors de la séance de la formation restreinte du 18 juin 2026 :

- Mme Anne DEBET, commissaire, entendue en son rapport ; En qualité de représentants de la société HOPITAL PRIVE DE LA LOIRE :

- [...] La société HOPITAL PRIVE DE LA LOIRE ayant été informée de son droit de garder le silence sur les faits qui lui étaient reprochés et ayant eu la parole en dernier ; La formation restreinte a adopté la décision suivante : I. FAITS ET PROCÉDURE A. Présentation de l'hôpital et des traitements mis en œuvre 1. La société HOPITAL PRIVE DE LA LOIRE (ci-après l'HOPITAL PRIVE DE LA LOIRE ou l'hôpital) est une société anonyme à conseil d'administration créée le 1er janvier 1970, immatriculée au RCS de Saint-Etienne sous le numéro 704 501 006 et domiciliée 39, boulevard de la Palle à Saint-Etienne (42100).

2. Issu du regroupement de quatre cliniques de l'agglomération de Saint-Etienne, l'hôpital a intégré en 2008 le groupe RAMSAY SANTE, qui se présente comme le leader de l'hospitalisation privée et des soins primaires en Europe et le 1er acteur de santé privé en France, Suède, Danemark et Norvège .

3. Entre les mois de juillet 2023 et juin 2024, l'hôpital a réalisé un chiffre d'affaires d'environ 91,8 millions d'euros, pour un résultat net déficitaire de 2,9 millions d'euros, et, entre juillet 2024 et juin 2025, un chiffre d'affaires d'environ 93,4 millions d'euros, pour un résultat net déficitaire de 5,2 millions d'euros. Le groupe RAMSAY a quant à lui réalisé, entre juillet 2024 et juin 2025, un chiffre d'affaires de [...], pour un résultat de [...].

4. L'hôpital propose l'ensemble des spécialités de soin (hors dialyse, neurochirurgie crânienne et chirurgie du cœur) et a accueilli en 2024 environ 50 000 patients. Il emploie 566 salariés en équivalent temps plein, dont une quinzaine de médecins, et dispose en sus d'une communauté médicale d'environ 200 praticiens libéraux (chirurgiens et médecins, kinésithérapeutes, sages-femmes), liés à l'hôpital par des contrats d'exercice.

5. L'ensemble des données des patients pris en charge au sein de l'hôpital est centralisé dans un dossier patient informatisé (ci-après, le DPI), qui permet de retracer leur parcours de soins, et de coordonner l'intervention des différents acteurs de soins (médecins, infirmiers, aides-soignants, paramédicaux notamment) en vue de la prise en charge et de l'administration des médicaments et des soins.

6. Sa gestion a lieu par l'intermédiaire du logiciel [...], qui se présente sous la forme d'une application web accessible à partir d'un navigateur, après saisie d'un identifiant et d'un mot de passe. Les fiches patients composant le DPI (qui contiennent l'ensemble des données relatives à chaque patient) peuvent être consultées, via cette application, à partir d'une adresse URL dans laquelle figure un identifiant propre au patient.

7. En 2025, le DPI de l'hôpital comportait les données à caractère personnel d'environ 530 000 patients, dont :

- des données de nature administrative : le numéro de dossier du patient, sa civilité, ses noms et prénoms, ses date et lieu de naissance, son sexe, son numéro de sécurité sociale, son adresse postale, son numéro d'identifiant patient permanent (ou IPP), sa situation de famille, sa situation professionnelle, l'identité et les coordonnées d'une personne de confiance à prévenir en cas de besoin et, dans certains cas, la copie du recto de la carte nationale d'identité du patient, de son tuteur/curateur ou de son responsable légal s'agissant des patients mineurs ;

- des données de nature biométrique : le cliché de sécurisation ;

- et des données concernant la santé : les observations soignantes, médicales et paramédicales, en amont et durant l'hospitalisation du patient.

8. L'accès au DPI était possible depuis le réseau interne de l'hôpital, mais également depuis l'extérieur :

- pour les salariés de la société HOPITAL PRIVE DE LA LOIRE disposant d'un poste informatique de l'hôpital et d'un accès à distance au moyen d'un VPN, ce qui correspondait à environ 40 personnes, notamment les cadres d'astreinte ;

- pour les utilisateurs externes à l'hôpital, à savoir les praticiens libéraux et leur secrétariat, et les salariés de la société éditrice du logiciel en charge de la maintenance du DPI. Ces utilisateurs externes se connectaient directement au DPI par le biais d'un accès à internet, sans connexion préalable à un VPN. Cela correspondait à environ 450 personnes.

9. Une matrice d'habilitation des droits d'accès au dossier patient informatisé de l'hôpital précisait les droits de chaque utilisateur sur les différents modules (données administratives, données de santé, etc.) en fonction de son profil. B. La violation de données à caractère personnel survenue en juin 2025 10. Le 1er juillet 2025, l'HOPITAL PRIVE DE LA LOIRE a été contacté par un praticien libéral rattaché à l'hôpital, qui indiquait ne plus parvenir à se connecter au DPI. A la suite de cette alerte, l'hôpital a conduit des investigations qui ont établi la survenance d'une violation de données.

11. Il résulte de ces investigations que l'attaquant est parvenu à se connecter au dossier patient informatisé de l'hôpital le 26 juin 2025, en utilisant les identifiants du compte d'un médecin libéral rattaché à l'hôpital. Il a alors multiplié les requêtes pour comprendre leur fonctionnement ainsi que l'arborescence du site.

12. Entre le 26 juin et le 1er juillet 2025, il a ensuite procédé à l'exfiltration de 524 867 fiches patients contenant des informations telles que l'état civil, le numéro de sécurité sociale, les coordonnées postales et électroniques et le numéro d'identifiant permanent des patients concernés. Parmi elles, 46 185 fiches comportaient également le recto de la carte nationale d'identité du patient ou de son représentant légal, 43 fiches comportaient des données de santé, et 202 246 fiches comportaient des données relatives à la personne de confiance désignée par le patient (lien de parenté, nom, prénom et numéro de téléphone).

13. L'HOPITAL PRIVE DE LA LOIRE a procédé à la notification de cette violation de données auprès de la Commission nationale de l'informatique et des libertés (ci-après, la CNIL ou la Commission) le 4 juillet 2025.

14. En parallèle, la CNIL a reçu neuf plaintes de personnes concernées par cette violation. C. La procédure suivie devant la CNIL 15. Le 29 juillet 2025, une délégation de la Commission a procédé à un contrôle sur place dans les locaux de l'hôpital, situés 39 boulevard de la Palle à Saint-Etienne (42100), afin de vérifier la conformité à 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 ou LIL), au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après le RGPD ou le Règlement) des traitements mis en œuvre. Le procès-verbal dressé à l'issue a été notifié à la société HOPITAL PRIVE DE LA LOIRE le 1er août 2025.

16. L'hôpital a communiqué des éléments complémentaires à la délégation de contrôle le 4 août 2025.

17. Aux fins d'instruction de ces éléments, la présidente de la Commission a, le 19 février 2026, désigné Mme Anne DEBET en qualité de rapporteure sur le fondement de l'article 22 de la loi du 6 janvier 1978 modifiée.

18. Le 5 mars 2026, à l'issue de son instruction, la rapporteure a fait signifier à la société HOPITAL PRIVE DE LA LOIRE un rapport détaillant les manquements aux articles 32 et 34 du RGPD qu'elle estimait constitués en l'espèce. Ce rapport proposait à la formation restreinte de la Commission de prononcer à l'encontre de la société une amende administrative, ainsi qu'une injonction de mettre en conformité ses pratiques avec les dispositions de l'article 32 du RGPD, assortie d'une astreinte. Il proposait également que cette décision soit rendue publique mais qu'il ne soit plus possible d'identifier nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.

19. Le 3 avril 2026, l'HOPITAL PRIVE DE LA LOIRE a produit des observations en réponse au rapport de sanction.

20. Le 18 mai 2026, la rapporteure a, en application du III de l'article 40 du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi Informatique et Libertés (ci-après, le décret du 29 mai 2019), informé l'hôpital que l'instruction était close.

21. Le même jour, l'hôpital a été informé que le dossier était inscrit à l'ordre du jour de la formation restreinte du 18 juin 2026.

22. La rapporteure et l'hôpital ont présenté des observations orales lors de la séance de la formation restreinte. II. MOTIFS DE LA DECISION A.

Sur la responsabilité de traitement de la société HOPITAL PRIVE DE LA LOIRE 23. En droit, l'article 4, paragraphe 7, du RGPD définit le responsable de traitement comme la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont

déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné (...) par le droit de l'Union ou par le droit d'un État membre .

24. En l'espèce, le traitement en cause est relatif au dossier patient informatisé (ou DPI), qui a pour finalité de centraliser l'ensemble des données à caractère personnel des patients pris en charge au sein de l'HOPITAL PRIVE DE LA LOIRE selon les modalités précédemment décrites.

25. La société HOPITAL PRIVE DE LA LOIRE a indiqué à la délégation être responsable des traitements de données à caractère personnel mis en œuvre dans le cadre de son DPI. L'hôpital est également désigné comme responsable de ces traitements dans le registre tenu au titre de l'article 30 du RGPD, ainsi que dans le contrat conclu avec la société [...], éditrice du logiciel [...] précité. Enfin, l'analyse d'impact sur la protection des données (ci-après l'AIPD), effectuée sur saisine de la correspondante RGPD de l'hôpital, confirme cette responsabilité, en explicitant les finalités du traitement, à savoir de permettre la tenue et la conservation du dossier informatisé du patient, dans les conditions prévues et imposées par le Code de la santé publique , et en en détaillant les moyens.

26. La formation restreinte rappelle que la tenue d'un dossier patient informatisé permet aux établissements de santé de répondre aux obligations de l'article R. 1112-2 du code de la santé publique, qui prévoit qu'un dossier médical est constitué pour chaque patient hospitalisé dans un établissement de santé public ou privé , et énumère les éléments devant y figurer.

27. Elle considère, au vu de ce qui précède et au regard des éléments du dossier, que l'hôpital est responsable des traitements relatifs au DPI, dont il a défini les finalités et les moyens essentiels. B.

Sur le manquement à l'obligation d'assurer la sécurité des données en application de l'article 32 du RGPD
28. En droit, l'article 32, paragraphe 1, du RGPD prévoit 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, (...) 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 (...) et notamment des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ainsi qu'une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement .

29. L'article 32, paragraphe 2, précise que lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite .

30. Il résulte de ces dispositions, lues à la lumière du considérant 75 du RGPD, que lorsque le traitement en cause porte sur des catégories particulières de données à caractère personnel, comme des données de santé, le traitement doit bénéficier de mesures de sécurité renforcées.

31. Par ailleurs, l'article L. 1470-2 du code de la santé publique, qui régit les services numériques en santé, prévoit que l'utilisation des services numériques en santé requiert l'identification électronique de leurs utilisateurs. Cette identification électronique repose sur un moyen, matériel ou immatériel, qui garantit un niveau adapté de sécurité et de protection des données à caractère personnel traitées par le service numérique en santé concerné.

32. Un référentiel, établi par arrêté des ministres chargés de la santé et de l'action sociale, détermine des catégories de services numériques en santé en fonction notamment des finalités du service, du type de données traitées, du nombre d'utilisateurs susceptibles d'accéder au service, de sa dimension nationale ou territoriale et, le cas échéant, de la circonstance que le service bénéficie à des utilisateurs professionnels de santé exerçant simultanément leur activité au sein de plusieurs personnes morales.

33. Ce référentiel précise, pour chaque catégorie d'utilisateurs et pour chaque catégorie de service numérique en santé : 1° Le niveau de garantie minimal exigé pour l'identification électronique, (...) 2° Pour les professionnels, le ou les moyens d'identification électronique exigés.

34. En application de ces dispositions, un arrêté du 28 mars 2022, entré en vigueur le 1er juin 2022, a approuvé et rendu opposable le référentiel de sécurité relatif à l'identification électronique des utilisateurs des services numériques en santé.

35. Il incombe ainsi au responsable de traitement de mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir la confidentialité et l'intégrité des données traitées, en tenant compte de la spécificité de ces données et du cadre juridique applicable aux services numériques en santé.

1. La portée de l'obligation de sécurité prévue à l'article 32 du RGPD 36. La formation restreinte rappelle tout d'abord que l'obligation de sécurité prévue par l'article 32 du RGPD est une obligation de moyens, qui impose au responsable du traitement de prendre des mesures qui, au regard des caractéristiques du traitement en cause, permettent à la fois de réduire la probabilité de la survenance d'une violation de données et le cas échéant, d'en atténuer la gravité. Il n'est donc pas attendu que les mesures de sécurité permettent d'éliminer toute forme de risque, et la simple survenance d'une violation de données ne caractérise pas à elle seule un manquement à l'article 32 du RGPD.

37. Cette analyse a été confirmée par la CJUE dans son arrêt du 14 décembre 2023 (CJUE, 14 décembre 2023, C-340/21, Agence nationale des recettes publiques de Bulgarie , points 29 à 31). La formation restreinte relève que, dans cet arrêt, la CJUE a retenu que la référence, figurant à l'article 32, paragraphes 1 et 2, du RGPD, à un niveau de sécurité adapté au risque et à un niveau de sécurité approprié témoigne de ce que ce règlement instaure un régime de gestion des risques et qu'il ne prétend nullement éliminer les risques de violations des données à caractère personnel. Ainsi, il ressort des libellés des articles 24 et 32 du RGPD que ces dispositions se bornent à imposer au responsable du traitement d'adopter des mesures techniques et organisationnelles destinées à éviter, dans toute la mesure du possible, toute violation de données à caractère personnel. Le caractère approprié de telles mesures doit être évalué de manière concrète, en examinant si ces mesures ont été mises en œuvre par ce responsable en tenant compte des différents critères visés auxdits articles et des besoins de protection des données spécifiquement inhérents au traitement concerné ainsi qu'aux risques induits par ce dernier. Partant, les articles 24 et 32 du RGPD ne sauraient être compris en ce sens qu'une divulgation non autorisée de données à caractère personnel ou un accès non autorisé à de telles données par un tiers suffisent pour conclure que les mesures adoptées par le responsable du traitement concerné n'étaient pas appropriées, au sens de ces dispositions, sans même permettre à ce dernier d'apporter la preuve contraire.

38. La CJUE a rappelé plus récemment que cette interprétation littérale est corroborée par une lecture combinée desdits articles 24 et 32 avec l'article 5, paragraphe 2, et l'article 82 dudit règlement, lus à la lumière des considérants 74, 76 et 83 de celui ci, dont il découle, en particulier, que le responsable du traitement est tenu d'atténuer les risques de violation des données à caractère personnel, et non d'empêcher toute violation de celles-ci (25 janvier 2024, C-687/21, point 39).

39. Dès lors, un manquement à l'obligation de sécurité peut être caractérisé indépendamment de l'existence d'une violation de données à caractère personnel.

40. La formation restreinte rappelle ensuite pouvoir sanctionner, non pas la survenance d'une violation de données, mais le fait que celle-ci a été rendue possible ou a été facilitée par l'absence ou l'insuffisance des mesures de sécurité mises en œuvre par un responsable du traitement, compte tenu de l'état de l'art. En ce sens, elle a déjà retenu, à plusieurs reprises, un manquement à l'article 32 du RGPD, compte tenu de l'absence ou de l'insuffisance des mesures de sécurité déployées qui a été exploitée par un attaquant dans le cadre d'une violation de données à caractère personnel (délibération

n° SAN-2021-020 du 28 décembre 2021 § 61 ; délibération de la formation restreinte n° SAN-2020-014 du 7 décembre 2020 § 19 ; délibération de la formation restreinte n° SAN – 2019-005 du 28 mai 2019 § 31 ; délibération n° SAN-2018-011 du 19 décembre 2018).

41. S'agissant de l'appréciation de l'obligation de moyens à laquelle est tenu le responsable de traitement, la CJUE considère que le caractère approprié de telles mesures techniques et organisationnelles doit s'apprécier en deux temps. D'une part, il convient d'identifier les risques de violation des données à caractère personnel induits par le traitement concerné et leurs éventuelles conséquences pour les droits et libertés des personnes physiques. Cette appréciation doit être conduite de manière concrète, en prenant en considération le degré de probabilité des risques identifiés et leur degré de gravité. D'autre part, il y a lieu de vérifier si les mesures mises en œuvre par le responsable du traitement sont adaptées à ces risques, compte tenu de l'état des connaissances, des coûts de mise en œuvre ainsi que de la nature, de la portée, du contexte et des finalités de ce traitement (14 décembre 2023, C 340/21, point 42).

42. Par conséquent, la formation restreinte n'entend pas sanctionner la violation de données en elle-même mais déterminer si, compte tenu de l'état des connaissances, des caractéristiques du traitement, de la probabilité et de la gravité des risques, ainsi que de la portée de l'obligation de sécurité précisée ci-dessus, la société HOPITAL PRIVE DE LA LOIRE a respecté ses obligations au titre de l'article 32 du RGPD en mettant en place des mesures techniques et organisationnelles appropriées. 2.

Sur les risques du traitement pour les personnes concernées 43. La formation restreinte rappelle que le considérant 75 du RGPD précise que des risques pour les droits et libertés des personnes physiques, dont le degré de probabilité et de gravité varie, peuvent résulter du traitement de données à caractère personnel qui est susceptible d'entraîner des dommages physiques, matériels ou un préjudice moral, en particulier : lorsque le traitement peut donner lieu à une discrimination, à un vol ou une usurpation d'identité, [...] à une perte de confidentialité de données protégées par le secret professionnel [...] ; lorsque le traitement concerne [...] des données concernant la santé [...] lorsque le traitement porte sur des données à caractère personnel relatives à des personnes physiques vulnérables, en particulier les enfants ; ou lorsque le traitement porte sur un volume important de données à caractère personnel et touche un nombre important de personnes concernées .

44. Le considérant 76 du RGPD énonce qu'il convient de déterminer la probabilité et la gravité du risque pour les droits et libertés de la personne concernée en fonction de la nature, de la portée, du contexte et des finalités du traitement. Le risque devrait faire l'objet d'une évaluation objective permettant de déterminer si les opérations de traitement des données comportent un risque ou un risque élevé .

45. Par ailleurs, le considérant 83 du RGPD précise que dans le cadre de l'évaluation des risques pour la sécurité des données, il convient de prendre en compte les risques que présente le traitement de données à caractère personnel, tels que la destruction, la perte ou l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite, qui sont susceptibles d'entraîner des dommages physiques, matériels ou un préjudice moral .

46. En l'espèce, les traitements liés au dossier patient informatisé de l'hôpital donnent accès à un ensemble de données permettant d'identifier très précisément les patients de l'hôpital, de connaitre leur âge, de les situer géographiquement et de les contacter, à savoir leurs nom, prénoms, date et lieu de naissance, numéro de sécurité sociale, numéro d'IPP, adresse postale, adresse électronique et numéro de téléphone, et d'en déduire que ces personnes ont fait l'objet d'une prise en charge hospitalière. Il peut également contenir la copie du recto de leur carte nationale d'identité, qui constitue un document officiel, ainsi que des données de santé particulièrement précises telles que le motif d'hospitalisation, la liste des consultations, et le cas échéant les informations relatives à leur anesthésie, qui sont des catégories particulières de données à caractère personnel au sens de l'article 9, paragraphe 1, du RGPD.

47. Par ailleurs, le DPI de l'hôpital permet d'accéder à un ensemble de données concernant des personnes désignées par des patients comme tiers de confiance, permettant, d'une part, de les identifier, de les situer, et de les contacter (l'hôpital ayant indiqué que les données habituellement renseignées pour ces personnes étaient leurs nom, prénoms, adresse postale et numéro de téléphone) et, d'autre part, de connaitre leur lien de parenté ou d'affection avec le patient de l'hôpital.

48. En 2025, le DPI de l'HOPITAL PRIVE DE LA LOIRE comportait les données d'environ 530 000 patients, outre celles d'environ 200 000 personnes désignées par ces derniers comme tiers de confiance.

49. La formation restreinte considère que l'accès non autorisé ou la divulgation des données contenues dans le DPI de l'hôpital est de nature à créer un préjudice moral et matériel pour les personnes concernées. En effet, celles-ci sont exposées à des risques liés à la revente de leurs données à des personnes malveillantes, à une usurpation de leur identité ou à des tentatives d'hameçonnage (pratique consistant à se faire passer pour un organisme connu de la personne concernée afin par exemple de lui demander ses coordonnées bancaires). La divulgation non autorisée de données de santé peut également avoir des conséquences lourdes dans la vie des personnes, notamment nuire à leur réputation et à leur intégrité, ou encore entrainer des risques de discrimination, par exemple dans les domaines de l'emploi, du logement ou encore de l'assurance.

50. Par ailleurs, la formation restreinte considère que le degré de probabilité que les risques de divulgation et d'accès non autorisé aux données traitées par l'hôpital se réalisent est élevé compte tenu de la recrudescence des violations de données depuis plusieurs années. En outre, le degré de probabilité que les risques liés à l'exploitation malveillante de ces données se réalisent en cas de perte de confidentialité est également élevé. Comme rappelé par le Groupement d'Intérêt Public Action contre la Cybermalveillance, l'hameçonnage est la menace prédominante en France (Cybermalveillance.gouv.fr dévoile les tendances de la menace cyber en France , 27 mars 2025).

51. La formation restreinte considère que, dans ces conditions, les mesures de sécurité mises en place par l'HOPITAL PRIVE DE LA LOIRE auraient dû permettre de répondre aux risques qui viennent d'être exposés. 3.

Sur le niveau de sécurité déployé par l'hôpital 52. L'Agence nationale de la sécurité des systèmes d'information (ci-après l'ANSSI) applique le principe de défense en profondeur aux systèmes d'information, qui consiste à ne pas faire reposer la sécurité sur un élément mais sur un ensemble cohérent. Cela signifie donc qu'il ne doit en théorie pas exister de point sur lequel tout l'édifice repose , c'est-à-dire que toute faille de sécurité potentielle d'un composant logiciel doit être compensée par au moins un second niveau de sécurité (voir le Memento sur le concept de défense en profondeur appliquée aux systèmes d'information, version 1.1 du 19 juillet 2004). L'ANSSI fait reposer ce concept sur le postulat que tout composant d'un système peut être défaillant ou compromis. Ce postulat, qui s'applique également aux fonctions de sécurité d'un SI [système d'information], est confirmé régulièrement par l'actualité sur les vulnérabilités de nombreux produits et logiciels (voir la note blanche Système d'information hybride et sécurité : un retour à la réalité, 10 août 2021).

53. En l'espèce, il appartient à la formation restreinte d'analyser si l'hôpital a mis en place un ensemble cohérent de mesures de sécurité pour protéger son système d'information. 3.1.

Sur les vulnérabilités ayant conduit ou facilité la survenance de la violation de données de juin 2025 3.1.1 Sur l'absence de sécurisation de l'accès à distance 54. Dans un contexte numérique, il est possible pour un professionnel de se connecter à distance (par exemple, depuis son domicile) au système d'information de sa structure au moyen de son ordinateur portable. Il s'agit de nomadisme numérique, que l'ANSSI définit comme toute forme d'utilisation des technologies de l'information permettant à un utilisateur d'accéder au SI [système d'information] de son entité d'appartenance ou d'emploi, depuis des lieux distants, ces lieux n'étant pas maîtrisés par l'entité (ANSSI, Recommandations sur le nomadisme numérique , 2018).

55. L'ANSSI relève, dans ses recommandations susmentionnées, que les lieux de travail non maîtrisés par une entité exposent celle-ci à des risques exacerbés de perte ou de vol de matériel, de compromission du matériel (par exemple, pendant une absence temporaire de l'utilisateur), de compromission des informations contenues dans le matériel volé, perdu ou emprunté, d'accès illégitime au système d'information de la société (et donc la compromission de celui-ci) et d'interception, voire d'altération des informations (perte de confidentialité ou d'intégrité).

56. Ainsi, elle souligne que dans le cadre du nomadisme, l'objectif est de réussir à s'aligner avec le niveau de sécurité du SI [système d'information] interne de l'entité, en répondant aux risques d'exposition plus forts listés ci-dessus , et considère que les entités doivent adopter des mesures spécifiques au nomadisme dans leurs politiques de sécurité du système d'information afin de réduire ou de couvrir les risques susvisés.

57. Elle précise qu'afin de permettre à un utilisateur d'accéder depuis un réseau non maitrisé à un système d'information interne, il est nécessaire de mettre en œuvre un canal qui établit un lien sécurisé entre le poste nomade et le système d'information interne de l'entité, au moyen de la technologie VPN (Virtual Private Network ou réseau privé virtuel).

58. En matière de santé, le référentiel de sécurité relatif à l'identification électronique des utilisateurs des services numériques en santé, rendu opposable par un arrêté du ministère des solidarités et de la santé du 28 mars 2022, prévoit que lorsqu'un professionnel accède à un service numérique depuis un poste connecté à Internet, en télétravail, en mobilité ou même sur le Wifi invité de l'établissement, la connexion est considérée comme un accès à distance. (...) L'authentification lors d'un accès à distance avec un moyen d'identification électronique de transition doit impérativement reposer sur deux facteurs de types différents parmi les trois suivants :

- connaissance : par exemple d'un mot de passe ;

- possession : par exemple d'un appareil fixe sur lequel s'effectue l'enregistrement ;

- biométrie : par exemple une empreinte digitale stockée et vérifiée sur un matériel en possession du professionnel.

59. Le référentiel propose ensuite une liste non exhaustive d'exemples de mécanismes d'authentification à deux facteurs permettant de garantir un niveau de sécurité suffisant, à savoir : un badge contenant une puce avec contact associée à un code PIN, un badge contenant une puce sans contact associée à un mot de passe, une clé de sécurité USB associée à un code PIN ou une empreinte digitale enregistrée sur la clé ou encore un mot de passe associé à un code TOTP (...) généré sur un matériel en possession de l'utilisateur, par exemple un téléphone ou un ordinateur pour lesquels il existe des applications compatibles et disponibles en libre accès .

60. Il précise également que l'ouverture du VPN par un moyen d'identification électronique à deux facteurs dispense toutefois d'exiger une authentification à deux facteurs pour les services accédés via ce VPN.

61. En l'espèce, la rapporteure reproche à l'hôpital de ne pas avoir mis en place des mesures appropriées pour sécuriser l'accès au DPI des utilisateurs externes qui, au moment de la violation de données, s'effectuait par internet, grâce à un identifiant et un mot de passe, sans connexion préalable à un VPN, ni moyen d'identification électronique à deux facteurs. Elle considère que cette carence de sécurité constitue un manquement à l'article 32 du RGPD et a rendu possible ou a minima facilité la survenance de la violation de données.

62. En défense, l'hôpital ne conteste pas que l'accès à distance des utilisateurs externes au DPI n'était pas sécurisé par une authentification à deux facteurs au moment de la violation de données, mais souligne que sa politique de mots de passe était conforme aux recommandations de la CNIL et de l'ANSSI. L'hôpital indique également qu'en concertation avec le groupe RAMSAY, il avait déjà planifié et

engagé, avant la violation de données, une trajectoire de sécurisation de l'accès à distance via une plateforme dotée d'une solution d'authentification multifacteur (la plateforme [...]), dont le déploiement a finalement été achevé en septembre 2025. En séance, l'hôpital a précisé qu'en 2024, au moment où l'évolution du logiciel [...] vers une version [...] aurait permis une authentification multifacteur, il a fait le choix de ne pas la déployer pour privilégier la solution [...]précédemment choisie par le groupe, qui serait déployée ultérieurement.

63. L'hôpital fait par ailleurs valoir ses efforts en vue de moderniser et d'améliorer son système d'information, étant officiellement engagé dans le programme HospiConnect piloté par l'Agence du numérique en santé, qui vise à atteindre les objectifs du référentiel d'identification électronique, ainsi que dans le programme Care.

64. La formation restreinte observe qu'au jour de la violation de données, environ 450 utilisateurs du DPI externes à l'hôpital, à savoir les praticiens libéraux liés à l'hôpital par des contrats d'exercice, leur secrétariat, ainsi que certains salariés de l'éditeur du logiciel [...], s'y connectaient à distance par le biais d'un simple accès internet, en saisissant un identifiant et un mot de passe, sans connexion préalable à un VPN ni moyen d'identification électronique à deux facteurs. Elle note que la version [...] du logiciel [...], déployée par l'hôpital au jour de la violation de données, proposait pourtant bien une authentification multifacteur, qui n'avait pas été mise en place.

65. La formation restreinte constate ainsi que l'accès à distance des utilisateurs externes n'était pas conforme aux exigences du référentiel précité, dès lors qu'il ne s'effectuait ni au moyen d'un VPN, ni avec un moyen d'identification électronique à deux facteurs.

66. Elle considère que l'absence d'authentification multifacteur lors de la connexion de ces utilisateurs au DPI de l'hôpital ne permettait pas d'assurer la sécurité du système d'information de la société. Elle souligne qu'en l'espèce, l'attaquant a exploité cette vulnérabilité pour accéder au dossier patient informatisé de l'hôpital et extraire les données qu'il contenait. Elle note en effet que, si ce dernier avait déployé une authentification multifacteur pour que les utilisateurs externes se connectent à son DPI, l'attaquant, disposant du mot de passe du compte d'utilisateur (facteur de connaissance), aurait également dû disposer d'un second facteur d'authentification. L'attaquant aurait alors été bloqué pour accéder au DPI de l'hôpital s'il ne disposait pas de ce second facteur d'authentification.

67. Il résulte de ce qui précède que, compte tenu de l'état des connaissances, des caractéristiques des traitements (qui concernent plusieurs centaines de milliers de données à caractère personnel, dont des données de santé) ainsi que des risques pour les droits et libertés des personnes physiques, l'hôpital n'a pas mis en œuvre un niveau de sécurité adapté.

68. Un manquement à l'article 32 du RGPD est ainsi caractérisé, faute pour l'hôpital d'avoir pris les mesures permettant d'assurer la sécurisation de l'accès à distance des utilisateurs externes au DPI.

69. La formation restreinte note que depuis la violation de données, l'hôpital a implémenté une authentification multifacteur pour la connexion des utilisateurs externes à son DPI, et s'est ainsi mis en conformité avec les règles précédemment rappelées. 3.1.2 Sur la politique d'habilitations inadéquate 70. En application de l'article 32 du RGPD, le responsable de traitement doit mettre en place des mesures appropriées pour assurer la confidentialité des données, et notamment éviter que ces dernières ne soient traitées de façon illicite par le fait de personnes qui n'ont pas besoin d'en connaitre.

71. La formation restreinte, dans sa délibération n° SAN-2021-019 du 29 octobre 2021, a ainsi rappelé que la gestion des habilitations à consulter ou à utiliser un système d'information doit tendre à limiter les accès aux seules données à caractère personnel dont un utilisateur a besoin pour l'accomplissement de ses missions, notamment en définissant des profils d'habilitation dans les systèmes en séparant les tâches et les domaines de responsabilité. Il appartient donc au responsable de traitement de mettre en place, en fonction de la plus ou moins grande diversité des missions des utilisateurs, une politique de gestion des habilitations qui soit appropriée à l'importance et à la sensibilité des données traitées, ainsi

qu'aux risques auxquels les personnes concernées sont exposées, en fonction des moyens dont il peut disposer.

72. En matière de santé, la Politique générale de sécurité des systèmes d'information de santé (ci-après dénommé PGSSI-S), élaborée par l'Agence du Numérique en Santé, fixe un cadre de référence destiné à sécuriser les pratiques de la e-santé pour les professionnels et les usagers du secteur sanitaire. En particulier, le guide de gestion des habilitations d'accès au système d'information rappelle que la notion d'équipe de soin doit être prise en compte dans la gestion des habilitations dans le respect de la loi et en fonction de l'organisation propre à la structure. Cette prise en compte peut constituer l'une des clés de définition des règles d'organisation et d'attribution des habilitations pour les personnels de santé .

73. Cette notion d' équipe de soins est définie par l'article L. 1110-12 du code de la santé publique comme un ensemble de professionnels qui participent directement au profit d'un même patient à la réalisation d'un acte diagnostique, thérapeutique, de compensation du handicap, de soulagement de la douleur ou de prévention de perte d'autonomie, ou aux actions nécessaires à la coordination de plusieurs de ces actes, et qui soit :

- exercent dans le même établissement de santé, au sein du service de santé des armées, dans le même établissement ou service social ou médico-social mentionné au I de l'article L. 312-1 du code de l'action sociale et des familles ou dans le cadre d'une structure de coopération, d'exercice partagé ou de coordination sanitaire ou médico-sociale figurant sur une liste fixée par décret ;

- se sont vu reconnaître la qualité de membre de l'équipe de soins par le patient qui s'adresse à eux pour la réalisation des consultations et des actes prescrits par un médecin auquel il a confié sa prise en charge ;

- exercent dans un ensemble, comprenant au moins un professionnel de santé, présentant une organisation formalisée et des pratiques conformes à un cahier des charges fixé par un arrêté du ministre chargé de la santé.

74. L'article L. 1110-4 du code de la santé publique prévoit par ailleurs que les professionnels de santé qui appartiennent à la même équipe de soins peuvent partager les informations concernant une même personne, sous réserve que ces informations soient strictement nécessaires à la coordination ou à la continuité des soins ou à son suivi médico-social et social. A l'inverse, la confidentialité de ces informations, couvertes par le secret médical, doit être assurée vis-à-vis des personnes qui n'ont pas à en connaître pour la prise en charge du patient.

75. Dès lors, le responsable de traitement d'un dispositif de dossiers patients informatisés doit mettre en place une politique d'habilitations rigoureuse et adaptée aux besoins de l'établissement, de sorte que chaque professionnel de santé et agent de l'établissement n'accède qu'aux dossiers dont il a à connaître. Cette politique d'habilitations doit combiner deux critères :

- d'une part, le métier exercé : ainsi, un agent responsable de l'accueil des patients dans la structure ne doit accéder qu'au dossier administratif du patient et non aux données médicales, alors qu'un médecin accèdera également aux données médicales ;

- d'autre part, la prise en compte de la notion d'équipe de soins, telle que définie par l'article L. 1110-12 du code de la santé publique, afin que seuls les professionnels effectivement impliqués dans la prise en charge d'un patient ou dans les soins qui lui sont prodigués puissent avoir accès aux informations couvertes par le secret médical.

76. Les habilitations accordées peuvent être complétées d'un mode bris de glace , défini par le référentiel d'authentification des acteurs de santé de la PGSSI-S comme l'attribution temporaire et exceptionnelle de droits étendus en situation de crise , permettant aux agents administratifs et professionnels de santé, en cas d'urgence, d'avoir accès à d'autres données pour tout patient. L'utilisation de ce mode bris de glace doit être particulièrement bien tracée et surveillée afin que toute

personne y ayant recours puisse être identifiée et justifier des conditions de son utilisation.

77. La rapporteure considère que la politique d'habilitations au DPI de l'hôpital est inadéquate dès lors qu'elle distingue certes différentes catégories de métiers et de services, en précisant les droits de chaque catégorie d'utilisateurs sur les différents modules du DPI (création, lecture, saisie/écriture ou administrateur), mais ne permet pas le cloisonnement des fiches patients accessibles à partir d'un compte d'utilisateur. Ainsi, les praticiens médicaux et paramédicaux peuvent librement accéder aux fiches de l'ensemble des patients de l'établissement, alors même qu'ils ne seraient pas impliqués dans leur prise en charge. Elle considère que ces faits constituent un manquement à l'article 32 du RGPD.

78. En défense, l'hôpital reconnait qu'au jour de la violation de données, le logiciel [...] ne permettait pas de réserver l'accès des dossiers patients à l'équipe de soins impliquée dans la prise en charge d'un patient donné. Il rappelle toutefois la réflexion menée pour formaliser une matrice d'habilitation distinguant les différents profils d'utilisateurs en fonction de leur métier, et limitant leurs droits d'accès aux seuls modules du DPI nécessaires à l'exercice de leurs fonctions. Il souligne la lourdeur d'un changement de logiciel de gestion du DPI sur les plans technique et organisationnel, et rappelle les efforts d'ores et déjà engagés pour moderniser et harmoniser son système d'information hospitalier.

79. La formation restreinte observe que la matrice d'habilitation des droits au sein du dossier patient informatisé de l'HOPITAL PRIVE DE LA LOIRE distingue différentes catégories de métiers et services selon leur nature (par exemple, médecins , pharmaciens , brancardiers ou service informatique), et précise les droits de chacune de ces catégories d'utilisateurs sur les différents modules du DPI (par exemple, prescriptions , planification bloc , brancardage , urgences). Elle constate toutefois que le logiciel ne propose pas le cloisonnement des fiches patients accessibles à partir d'un compte d'utilisateur, ce qui permet aux praticiens médicaux et paramédicaux d'accéder librement aux données à caractère personnel de l'ensemble des patients de l'hôpital (pour les données contenues dans les modules auxquels ils peuvent accéder), quand bien même ils n'auraient pas été ou ne seraient pas personnellement impliqués dans leur prise en charge.

80. La formation restreinte observe également que la matrice d'habilitation des droits, telle que formalisée par l'hôpital, conduit à ce que les salariés de la société éditrice du logiciel en charge de la maintenance du DPI puissent, en l'absence de cloisonnement des dossiers patients, accéder eux aussi à l'intégralité des dossiers des patients de l'hôpital.

81. Elle note ainsi que, si la politique d'habilitations définie par l'hôpital peut correspondre au premier critère, s'agissant du type de métier exercé (un médecin pouvant par exemple accéder aux données médicales des patients, alors que le personnel de l'accueil ne peut accéder qu'au module mouvements), elle n'est pas satisfaisante s'agissant du second critère, relatif à la notion d'équipe de soins telle que définie par l'article L. 1110-12 du code de la santé publique.

82. Elle considère qu'un tel accès élargi aux données à caractère personnel des patients de l'hôpital, notamment à leurs données de santé, ne trouve aucune justification, et que la matrice d'habilitation des droits au DPI de l'hôpital n'est dès lors pas satisfaisante au regard des dispositions de l'article L. 1110-4 du code de la santé publique précitées, et de la notion d'équipe de soins définie par l'article L. 1110-2 de ce code.

83. La formation restreinte rappelle que les habilitations d'accès au DPI doivent en effet être configurées de telle sorte que seuls les professionnels du secteur médical ou paramédical effectivement impliqués dans la prise en charge d'un patient ou dans les soins qui lui sont prodigués aient accès aux informations couvertes par le secret médical. Ces limitations d'accès peuvent être complétées par des habilitations attribuées temporairement et tracées, afin de répondre aux situations d'urgence pour lesquelles un professionnel de santé doit intervenir alors qu'il n'est pas membre de l'équipe de soins (par exemple, en cas d'urgence, via un accès de type bris de glace permettant l'attribution temporaire et exceptionnelle de droits étendus).

84. Elle observe que l'analyse d'impact sur la protection des données réalisée par l'HOPITAL PRIVE DE LA LOIRE en 2021 avait d'ores et déjà identifié ce défaut de sécurité issu de l'absence de cloisonnement des dossiers patients comme la principale menace pouvant permettre un accès illégitime aux données, notamment en cas de piratage externe, malveillance interne, erreur humaine interne , avant de conclure que si la gravité du risque était maximale , sa vraisemblance était toutefois jugée limitée .

85. La formation restreinte considère ainsi que le manquement de l'hôpital à son obligation d'assurer la sécurité et la confidentialité du traitement est pleinement caractérisé. Elle souligne que cette carence de sécurité a directement contribué à l'ampleur de la violation de données, dès lors qu'en utilisant les identifiants d'un compte de médecin pour se connecter au DPI, l'attaquant a pu, en l'absence de cloisonnement des dossiers patients, accéder aux données de l'intégralité des patients de l'hôpital, et in fine les extraire. A contrario, si un tel cloisonnement avait été mis en œuvre, la fuite de données aurait été limitée aux seuls dossiers de patients effectivement pris en charge par le médecin dont les identifiants avaient été dérobés.

86. En dernier lieu, la formation restreinte observe que les limites techniques du logiciel [...], qui ne prévoit pas le cloisonnement des dossiers patients ni de mode bris de glace , ne sont pas un fait exonératoire pour l'hôpital, le responsable de traitement se devant de choisir un outil à jour de l'état de l'art et présentant des garanties de sécurité suffisantes.

87. Un manquement à l'article 32 du RGPD est dès lors constitué, eu égard à la mise en place par l'hôpital d'une politique d'habilitations inadéquate, sans cloisonnement des dossiers patients. 3.1.3 Sur l'insuffisance des mesures de traçabilité 88. Dans sa délibération n° 2021-122 du 14 octobre 2021 portant adoption d'une recommandation relative à la journalisation, la CNIL rappelle que la mise en place d'un dispositif de journalisation participe au respect de l'obligation de sécurisation de tout traitement de données à caractère personnel, en application des articles 5 et 32 du RGPD .

89. Elle recommande ainsi aux organismes de collecter des informations sur les personnes administrant ou accédant à leurs ressources, comme l'identifiant de l'utilisateur, la date et l'heure de l'accès et l'identifiant de l'équipement utilisé et précise que cette sécurisation est essentiellement active : elle repose sur une exploitation en temps réel ou à court terme de ces données pour détecter des opérations anormales afin de parer des attaques ou intrusions, ou de remédier rapidement à un incident informatique en facilitant l'identification du problème .

90. L'Agence nationale de la sécurité des systèmes d'information (ci-après l'ANSSI), rappelle quant à elle dans ses Recommandations de sécurité pour l'architecture d'un système de journalisation du 28 janvier 2022, que l'analyse continue des journaux d'évènements permet de repérer des activités inhabituelles, tandis que l'archivage des journaux rend possible les levées de doutes a posteriori. En ce sens, la journalisation constitue également le prérequis indispensable à la mise en œuvre d'une capacité de détection, d'analyse et de réponse aux incidents de sécurité .

91. L'ANSSI y dresse la liste des catégories d'évènements devant être collectées pour constituer un socle minimal de journalisation, parmi lesquelles, en matière d'authentification, les ouvertures de sessions et les réussites et échecs des authentifications, et en matière d'accès aux ressources sensibles, les accès ou tentatives d'accès en lecture/écriture/exécution/suppression aux ressources sensibles.

92. Il découle de ce qui précède que la simple collecte des données de journalisation ne suffit pas à sécuriser un système d'information. Le dispositif de journalisation n'est en effet efficace que si une entité est en capacité de traiter les informations enregistrées dans les journaux afin d'être en mesure, le cas échéant, de détecter rapidement un comportement suspect.

93. Le Comité européen de la protection des données considère également dans ses lignes directrices 9/2022 sur la notification de violations de données à caractère personnel en vertu du RGPD, que la capacité de détecter une violation, d'y remédier et de la communiquer dans les meilleurs délais devrait

être considérée comme un élément essentiel .

94. En l'espèce, la rapporteure reproche à l'hôpital de n'avoir pris aucune mesure d'analyse automatisée des traces applicatives du DPI, aux fins de détecter, en temps réel ou à très court terme, une activité suspecte et, le cas échéant, de déclencher un mécanisme d'alerte. Elle note que cette carence de surveillance a permis à l'attaquant d'effectuer un nombre extrêmement élevé de requêtes au sein du DPI de l'hôpital pendant près d'une semaine, entre le 26 juin et le 1er juillet 2025, et d'extraire les données de 524 867 patients, sans que ce comportement anormal ne soit détecté.

95. En défense, l'hôpital conteste partiellement la caractérisation de ce manquement et reproche au rapport de ne pas rendre compte de l'ensemble des moyens de supervision mis en place, à savoir un logiciel de détection et de réponse sur les postes de travail et les serveurs (EDR), un centre des opérations de sécurité (SOC), un système de supervision sur base de la solution [...], et un système de journalisation avec enregistrement des traces applicatives. Il indique que si ces outils de détection n'ont généré aucune alerte durant l'attaque, c'est parce que la charge générée par les requêtes de l'attaquant n'a pas modifié de manière significative le seuil d'utilisation habituel.

96. Il concède cependant qu'au moment de la violation de données, il n'existait pas d'analyse automatique en temps réel des traces applicatives du DPI, et indique avoir depuis mis en place un certain nombre de mesures pour permettre la détection d'anomalies volumétriques ou comportementales significatives.

97. La formation restreinte relève qu'au moment de la violation de données, l'hôpital disposait bien d'équipements de détection de menaces de sécurité informatique et d'un centre des opérations de sécurité visant à traiter les données issues notamment des équipements réseaux et de l'Active directory.

98. S'il disposait également d'un système permettant de consigner les actions réalisées par les utilisateurs du DPI (connexion, création, modification ou suppression de données, etc.), aux fins d'en conserver une trace (ces journaux d'événements étant appelés les traces applicatives), il ressort toutefois des éléments du dossier que ces traces ne faisaient l'objet d'aucune analyse automatisée ni d'aucun contrôle régulier, et n'étaient exploitées qu'à la demande, par exemple en cas de suspicion d'une anomalie. La formation restreinte relève ainsi qu'aucune mesure ne permettait de détecter ni de signaler, en temps réel ou à court terme, une activité suspecte au sein du DPI (par exemple, des accès susceptibles d'être frauduleux ou illégitimes ou la consultation d'un volume anormalement élevé de dossiers patients).

99. La formation restreinte considère que les dispositifs de sécurité mis en place par l'hôpital, dont l'existence n'est pas contestée, étaient dès lors insuffisants pour garantir la sécurité et la confidentialité des données du traitement.

100. Elle observe que cette carence de surveillance a directement contribué à l'ampleur de la violation intervenue, l'attaquant ayant pu effectuer un nombre extrêmement élevé de requêtes au sein du DPI de l'hôpital entre le 26 juin et le 1er juillet 2025, et extraire un volume très important de données, sans que ce comportement anormal du compte utilisateur ne soit détecté, seul le signalement d'un utilisateur ayant permis de révéler la violation de données.

101. Elle note que l'analyse effectuée a posteriori a, quant à elle, permis d'identifier les signes manifestes d'une activité anormale sur le compte, à savoir tout d'abord une phase de reconnaissance manuelle d'une durée d'environ 12 heures, au cours de laquelle l'attaquant a réalisé 665 requêtes afin de comprendre leur fonctionnement, l'arborescence du site, et d'identifier les données disponibles, puis une phase d'extraction automatique, qui a conduit à l'appréhension de 524 867 fiches de patients sur une durée de cinq jours, ce qui correspond à une moyenne de 73 fiches de patients consultées par minute. Elle souligne que si l'activité réseau générée par l'attaquant n'était pas suffisamment importante pour être détectée par les outils d'analyse de charge déployés par l'hôpital, la mise en place d'un système de

journalisation efficient, avec un enregistrement et une analyse automatique des traces applicatives, aurait pu permettre de déceler, en temps réel ou à court terme, le volume anormalement élevé de consultation de dossiers à partir du même compte d'utilisateur, incompatible avec une activité humaine, et de mettre fin au plus vite à l'exfiltration de données.

102. La formation restreinte considère ainsi qu'au regard de cette insuffisance des mesures de traçabilité, le manquement à l'article 32 du RGPD est caractérisé.

103. Elle relève que depuis la violation de données, l'hôpital a adopté un certain nombre de mesures afin de mettre son système informatique en conformité, et de permettre la détection d'anomalies volumétriques ou comportementales au sein de son DPI. 3.2.

Sur les autres vulnérabilités détectées lors des opérations de contrôle 3.2.1 Sur le non-respect du secret des mots de passe dans le cadre de la procédure de réinitialisation ayant fait suite à la violation de données 104. En application de l'article 32 du RGPD, les responsables de traitement sont tenus de mettre en place une politique d'authentification robuste, qui constitue une mesure élémentaire de sécurité. Lorsque le mot de passe n'est pas défini par l'utilisateur mais lui est transmis par le responsable de traitement, celui-ci doit sécuriser la transmission de cette information personnelle et confidentielle.

105. Dans sa délibération n° 2022-100 du 21 juillet 2022 portant adoption d'une recommandation relative aux mots de passe et autres secrets partagés – qui n'a certes pas un caractère impératif mais qui fournit un éclairage pertinent sur les mesures qu'il convient de prendre en matière de sécurité – la Commission liste un certain nombre de précautions à adopter lors de la transmission d'un mot de passe, afin de garantir que seul l'utilisateur concerné soit en possession de celui-ci. Ces précautions s'appliquent également dans l'hypothèse d'un renouvellement de mot de passe.

106. Dès lors, des modalités de transmission d'un mot de passe, même temporaire, qui ne permettraient pas de garantir sa confidentialité à l'égard de tiers, ne seraient pas conformes aux exigences de l'article 32 du RGPD.

107. La rapporteure considère que la procédure de réinitialisation des mots de passe des usagers du DPI externes à l'hôpital, mise en œuvre à la suite de la violation de données, ne s'est pas effectuée dans des conditions permettant de garantir leur confidentialité, dès lors qu'elle a consisté à attribuer un mot de passe temporaire identique à l'ensemble des praticiens, qui de surcroit ne leur a pas été transmis directement, mais a été communiqué au président de la commission médicale d'établissement, à charge pour lui de le leur retransmettre. Elle estime que cette carence de sécurité constitue un manquement à l'article 32 du RGPD.

108. En défense, l'hôpital reconnait avoir attribué le même mot de passe temporaire à l'ensemble des praticiens externes, mais insiste sur le caractère d'urgence de cette mesure, qui visait à stopper la violation en cours sans mettre en péril la continuité des soins, alors que le logiciel [...] ne permettait pas de demander une réinitialisation individuelle des mots de passe de manière automatisée. Il estime ainsi qu'il s'agissait de la seule solution technique disponible.

109. La formation restreinte relève qu'à la suite de la détection de la violation de données, l'HOPITAL PRIVE DE LA LOIRE a procédé à la réinitialisation des mots de passe de l'ensemble des usagers du DPI externes à l'hôpital, cette procédure ayant consisté à remplacer leur mot de passe de connexion par un mot de passe temporaire, identique pour tous, et à le communiquer au président de la commission médicale d'établissement, à charge pour lui de le leur retransmettre. Lors de leur première connexion au DPI au moyen de ce mot de passe temporaire, les utilisateurs étaient invités à le modifier en adoptant un mot de passe qui leur soit personnel. Ce mot de passe temporaire ayant une durée de validité d'une semaine, les utilisateurs qui ne s'étaient pas connectés au DPI dans ce délai pour réinitialiser leur mot de passe étaient invités à se rendre physiquement au service informatique de l'hôpital.

110. La formation restreinte observe qu'en prévoyant le même mot de passe temporaire pour l'ensemble des utilisateurs du DPI externes à l'hôpital, et en le leur transmettant par l'intermédiaire du président de la commission médicale d'établissement, l'hôpital n'a pas respecté le secret des mots de passe, qui doivent être confidentiels et personnels à chaque utilisateur. Il a au demeurant fourni à l'ensemble des utilisateurs les moyens de se connecter à des comptes de tiers, dès lors que tous avaient durant plusieurs jours le même mot de passe, et d'accéder ainsi à toutes les données à caractère personnel auxquels ces tiers pouvaient accéder.

111. Dès lors, elle considère que la transmission d'un mot de passe temporaire identique pour l'ensemble des utilisateurs, qui plus est par l'intermédiaire d'un tiers, ne permettait pas de garantir la confidentialité des données traitées, et que ces faits ont dès lors constitué un manquement à l'article 32 du RGPD. La formation restreinte observe que cette pratique démontre la négligence de l'hôpital, alors même que ce dernier faisait face à une violation de données mettant en lumière plusieurs carences de sécurité.

112. Elle précise que les éventuelles limites techniques du logiciel utilisé ne constituent pas un fait exonératoire pour le responsable de traitement, ce dernier devant s'assurer que l'outil choisi est conforme à l'état de l'art et permet d'assurer la sécurité et la confidentialité du traitement dans le respect de l'article 32 du RGPD. 3.2.2 Sur l'absence de contrôle de l'accès de l'éditeur du logiciel aux données du traitement 113. Le responsable de traitement devant mettre en place des mesures appropriées pour assurer la confidentialité des données et éviter que ces dernières ne soient traitées de façon illicite par des personnes qui n'ont pas besoin d'en connaître (cf supra, §70), l'une des précautions élémentaires doit consister à limiter l'accès aux données aux utilisateurs en ayant besoin pour l'accomplissement de leurs missions, à travers une gestion des habilitations.

114. De plus, au regard du considérant 75 du RGPD, qui éclaire la portée à donner à l'article 32 susvisé, lorsque le traitement en cause porte sur des catégories particulières de données à caractère personnel, comme des données de santé, le traitement doit bénéficier de mesures de sécurité renforcées.

115. Dans son guide relatif à l'administration sécurisé des systèmes d'information, l'ANSSI rappelle qu'une entité peut faire appel à des tiers, tels que des constructeurs d'équipements, éditeurs de logiciels, etc. Les besoins d'accès de ces tiers aux systèmes d'information peuvent être réguliers (par exemple dans le cadre d'un contrat d'infogérance) ou ponctuels (par exemple dans le cadre d'un contrat de support). L'accès au système d'information de l'entité, généralement à distance, constitue alors un risque majeur de compromission. Il est donc primordial de fixer un cadre relatif à ces accès.

116. La rapporteure reproche à l'hôpital d'avoir laissé à la société éditrice du logiciel [...] un accès à distance permanent au DPI, et par conséquent aux données à caractère personnel des patients, sans qu'aucune action ni autorisation préalable de l'hôpital ne lui soit nécessaire. La rapporteure considère que cet accès permanent et sans contrôle au DPI de l'hôpital ne permet pas d'assurer la confidentialité du traitement, et caractérise ainsi un manquement à l'article 32 du RGPD.

117. En défense, l'hôpital considère que l'accès permanent de l'éditeur du logiciel répond à un principe de tierce maintenance applicative visant à assurer un support rapide et efficace. Il précise que l'accès permanent au DPI, via l'application web, ne concernait pas l'ensemble des interventions de l'éditeur, mais seulement les interventions de maintenance, toute action d'administration technique avancée nécessitant quant à elle une connexion via le serveur bastion de la société, sur lequel toute activité est tracée en détail.

118. L'hôpital ajoute que depuis la violation de données, des mesures correctrices ont été prises afin que l'éditeur ne puisse se connecter au DPI qu'au travers du serveur bastion ; de plus, les comptes d'utilisateur fournis à ce prestataire sont gérés par une solution de gestion des identités centralisées, et sont désactivés d'office tous les 180 jours.

119. La formation restreinte relève que la société éditrice du logiciel dispose d'un accès permanent au DPI de l'hôpital, notamment à des fins de maintenance de cette solution informatique, par le biais de

mises à jour et de tests fonctionnels. Elle note que les opérations de contrôle ont permis de préciser que les salariés de cette société en charge de la maintenance du DPI de l'hôpital pouvaient initialement y accéder selon deux modalités : soit depuis l'application [...], au moyen d'un compte d'utilisateur propre à chaque salarié, donnant accès tant aux paramétrages du logiciel qu'aux données des patients, soit depuis un serveur bastion , donnant accès par rebond au serveur applicatif et au serveur de bases de données du DPI, chaque salarié disposant d'un compte nominatif sur le serveur bastion.

120. La formation restreinte constate ainsi que les salariés de la société éditrice du logiciel [...] peuvent accéder au DPI de l'hôpital à leur initiative, sans devoir solliciter l'autorisation préalable de l'hôpital ni même le prévenir.

121. La formation restreinte considère qu'une telle prérogative d'accès permanent et sans contrôle au DPI de l'hôpital, et par voie de conséquence aux données à caractère personnel des patients, n'est pas nécessaire au regard de la mission d'assistance technique et de maintenance de la société éditrice du logiciel. Au contraire, dans l'hypothèse où une opération de maintenance aurait effectivement nécessité un accès au DPI de l'hôpital, les salariés de l'éditeur du logiciel auraient dû systématiquement solliciter l'autorisation préalable de l'hôpital.

122. Dès lors, la formation restreinte considère qu'en permettant à la société éditrice du logiciel [...] d'accéder au DPI de sa propre initiative, sans limitation d'accès ni autorisation préalable, l'hôpital lui a octroyé des droits dépassant les nécessités de sa mission, et ne permettant pas d'assurer la confidentialité et la sécurité des données traitées, ce qui caractérise un manquement à l'article 32 du RGPD.

123. La formation restreinte observe à cet égard que le fait que les salariés de la société éditrice ne puissent désormais se connecter au DPI qu'au travers d'un serveur bastion n'est pas de nature à faire cesser ce manquement, qui concerne l'habilitation de ces salariés à accéder aux données du DPI, et non la sécurisation de leur accès à distance. Ainsi, seules des mesures techniques visant à empêcher tout accès de la société éditrice du logiciel [...] au DPI, sauf à ce que l'hôpital lève cette contrainte technique (par exemple, une validation manuelle de l'accès au DPI sur le serveur bastion), pourrait permettre à l'hôpital de se mettre en conformité. C.

Sur le manquement à l'obligation de communiquer aux personnes concernées la violation de données à caractère personnel en application de l'article 34 du RGPD 124. En droit, aux termes de l'article 34, paragraphe 1, du RGPD, lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais .

125. Il appartient ainsi au responsable de traitement d'évaluer le risque encouru par les personnes concernées et de procéder, le cas échéant, à l'information des personnes.

126. S'agissant de l'évaluation du risque, les lignes directrices 9/2022 sur la notification de violations de données à caractère personnel en vertu du RGPD, adoptées par le Comité européen de la protection des données (ci-après le CEPD) le 28 mars 2023, prévoient que différents facteurs sont à prendre en compte : le type de violation, la nature, le caractère sensible et le volume des données à caractère personnel, la facilité d'identification des personnes concernées, la gravité des conséquences pour les personnes concernées, les caractéristiques particulières des personnes concernées, les caractéristiques particulières du responsable du traitement et le nombre de personnes concernées.

127. Ces lignes directrices précisent également qu'un risque pour les droits et libertés des individus existe lorsqu'une violation est susceptible d'engendrer des dommages physiques, matériels ou un préjudice moral pour les personnes dont les données ont fait l'objet de la violation. Des exemples de tels dommages sont la discrimination, le vol ou l'usurpation d'identité, la perte financière ou l'atteinte à la réputation . De plus, le fait que le responsable du traitement ait connaissance ou non de ce que des

données à caractère personnel se trouvent en la possession de personnes dont les intentions sont inconnues ou potentiellement malicieuses peut avoir une incidence sur le niveau de risque potentiel. Ainsi, en fonction de la nature de la violation et des risques engendrés, une communication rapide aidera les personnes concernées à prendre des mesures pour se protéger contre toute conséquence négative de la violation.

128. S'agissant du contenu de l'information à délivrer, l'article 34, paragraphe 2, du RGPD énumère les mentions devant obligatoirement figurer dans le contenu de cette communication. Celle-ci doit contenir une description de la nature de la violation de données à caractère personnel, de ses conséquences probables, ainsi que des 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. Par ailleurs, elle doit 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.

129. Le considérant 86 du RGPD précise que cette communication doit formuler des recommandations à la personne physique concernée pour atténuer les effets négatifs potentiels puisque son objectif est de permettre aux personnes concernées de prendre les précautions qui s'imposent .

130. Enfin, les lignes directrices 9/2022 précitées rappellent qu'en principe, la violation devrait être communiquée aux personnes concernées directement (…) Une notification se limitant uniquement à un communiqué de presse ou à un blog d'entreprise ne constituerait pas une méthode efficace de communication d'une violation à une personne. Le CEPD recommande que les responsables du traitement choisissent une méthode qui maximise la probabilité que les informations soient communiquées comme il se doit à toutes les personnes concernées. En fonction des circonstances, cela peut impliquer que le responsable de traitement ait recours à plusieurs méthodes de communication, par opposition à un canal de contact unique.

131. La rapporteure considère que l'hôpital a commis un manquement à l'article 34 du RGPD dès lors que seuls ses patients ont été informés de la violation de données intervenue, et qu'aucune information directe n'a été délivrée aux 202 246 personnes désignées par des patients comme tiers de confiance, alors même que leurs données à caractère personnel ont également été appréhendées par l'attaquant lorsqu'il a procédé à l'extraction des fiches patients du DPI.

132. En défense, l'hôpital conteste le manquement reproché.

133. Il rappelle tout d'abord les diligences accomplies en vue de contacter ses patients selon des modalités différenciées et adaptées aux données appréhendées, par le biais d'un communiqué de presse sur son site web, de 126 000 courriels personnalisés en fonction de la nature des données compromises, de 210 000 SMS adressés aux patients dont l'adresse électronique était inconnue, et de 88 000 courriers postaux adressés à ceux dont l'adresse électronique et le numéro de portable n'étaient pas disponibles.

134. Il conteste la présentation faite par le rapport de la nature et du volume des données à caractère personnel concernant des tiers de confiance, et indique que ces données seraient parcellaires, et se limiteraient habituellement aux nom, prénom, numéro de téléphone, lien de parenté avec le patient, et à la mention confiance oui/non . Il indique également que ces données ne sont pas présentées de manière structurée dans l'extraction réalisée par la société éditrice du logiciel Expert Santé , ce qui en limite l'exploitabilité.

135. L'hôpital fait ainsi valoir qu'au terme de son analyse de risques, il a estimé que la violation des données des personnes de confiance ne présentait pas de risques élevés à leur égard, et ne nécessitait dès lors pas une communication au titre de l'article 34 du RGPD, compte tenu du caractère parcellaire des informations les concernant, de l'absence de sensibilité des données et de l'absence de vulnérabilité des personnes concernées.

136. La formation restreinte relève que l'hôpital a contacté ses patients par différents biais afin de les informer de la survenance d'une attaque informatique (communiqué de presse sur la page d'accueil de son site web, courriels, SMS, courriers postaux), et qu'ainsi la communication réalisée à destination de ces personnes est conforme aux exigences posées par l'article 34 du RGPD.

137. Elle relève qu'en revanche, aucune information n'a été délivrée aux 202 246 personnes désignées comme tiers de confiance par des patients de l'hôpital, alors même que leurs données à caractère personnel ont également été appréhendées par l'attaquant à l'issue de la violation.

138. Elle précise que la communication aux personnes concernées par une violation de données devant par principe être effectuée de manière directe, le communiqué de presse diffusé sur le site web de l'hôpital ne saurait être considéré comme suffisant au regard de l'article 34 du RGPD. Elle observe à cet égard que les personnes désignées comme tiers de confiance n'ayant pas été prises en charge elles-mêmes au sein de l'hôpital, elles avaient d'autant moins de raison de consulter spontanément ce site web.

139. Or, la formation restreinte considère que la violation de données survenue entre le 26 juin et le 1er juillet 2025 expose bien ces personnes à des risques importants, dès lors que les informations appréhendées, en l'occurrence leurs noms, prénoms, numéro de téléphone et lien de parenté avec un patient, peuvent être utilisées à des fins frauduleuses, par exemple dans le cadre de campagnes d'hameçonnage. De plus, la formation restreinte souligne que ces informations concernant les tiers de confiance doivent être envisagées en lien avec celles du patient auquel elles sont rattachées dans la fiche patient, et constituent ainsi un ensemble de données pouvant être réutilisé dans le cadre d'usurpations d'identités, notamment pour tenter d'effectuer des formalités administratives au nom d'un patient décédé. Ce risque apparait d'autant plus important que certaines fiches patient récupérées par l'attaquant comportent un volume d'informations important, avec pour certaines des données de santé particulièrement précises, relatives à des hospitalisations actuelles ou passées, et pour 46 185 d'entre elles la copie du recto de la carte nationale d'identité du patient.

140. La formation restreinte observe que l'hôpital a été en mesure de quantifier et d'identifier précisément les personnes désignées tiers de confiance dès le 7 juillet 2025, date à laquelle il a notifié la violation de données à la CNIL. En outre, s'il ne disposait pas de leur adresse électronique ou de leur adresse postale, l'hôpital aurait pu les contacter en leur adressant un SMS sur leur téléphone portable, généralement renseigné, comme il l'a fait pour les patients concernés par la violation.

141. Il résulte de ce qui précède qu'en s'abstenant d'informer les 202 246 personnes désignées comme tiers de confiance par des patients de la survenance d'une attaque informatique ayant permis l'appréhension frauduleuse de leurs données à caractère personnel, l'HOPITAL PRIVE DE LA LOIRE a commis un manquement à l'article 34 du RGPD. III. SUR LES MESURES CORRECTRICES ET LEUR PUBLICITÉ 142. En droit, aux termes de l'article 20-IV de la loi n° 78-17 du 6 janvier 1978 modifiée, 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 (...) 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 .

143. L'article 83 du RGPD prévoit en outre que 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 , avant de

préciser les éléments devant être pris en compte pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de cette amende.

144. Le considérant 150 du RGPD précise que lorsque des amendes administratives sont imposées à une entreprise, ce terme doit, à cette fin, être compris comme une entreprise conformément aux articles 101 et 102 du traité sur le fonctionnement de l'Union européenne .

145. Les lignes directrices sur l'application et la fixation des amendes administratives aux fins du règlement 2016/679 indiquent quant à elles que la notion d'entreprise doit s'entendre comme une unité économique pouvant être formée par la société mère et toutes les filiales concernées. Conformément au droit et à la jurisprudence de l'Union, il y a lieu d'entendre par entreprise l'unité économique engagée dans des activités commerciales ou économiques, quelle que soit la personne morale impliquée .

146. Par un arrêt du 5 décembre 2023 (CJUE, grande chambre, C-807/21, Deutsche Wohnen), la CUJE a considéré, s'agissant de la notion d'entreprise qu'ainsi que l'a relevé M. l'avocat général au point 45 de ses conclusions, c'est dans ce contexte spécifique du calcul des amendes administratives imposées pour des violations visées à l'article 83, paragraphes 4 à 6, du RGPD qu'il y a lieu d'appréhender le renvoi, effectué au considérant 150 de ce règlement, à la notion d'entreprise , au sens des articles 101 et 102 TFUE. À cet égard, il convient de souligner que, aux fins de l'application des règles de la concurrence, visées par les articles 101 et 102 TFUE, cette notion comprend toute entité exerçant une activité économique, indépendamment du statut juridique de cette entité et de son mode de financement. Elle désigne ainsi une unité économique même si, du point de vue juridique, cette unité économique est constituée de plusieurs personnes physiques ou morales. Cette unité économique consiste en une organisation unitaire d'éléments personnels, matériels et immatériels poursuivant de façon durable un but économique déterminé (arrêt du 6 octobre 2021, Sumal, C 882/19, EU:C:2021:800, point 41 et jurisprudence citée). Ainsi, il ressort de l'article 83, paragraphes 4 à 6, du RGPD, qui vise le calcul des amendes administratives pour les violations énumérées dans ces paragraphes, que, dans le cas où le destinataire de l'amende administrative est ou fait partie d'une entreprise, au sens des articles 101 et 102 TFUE, le montant maximal de l'amende administrative est calculé sur la base d'un pourcentage du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise concernée. En définitive, ainsi que M. l'avocat général l'a relevé au point 47 de ses conclusions, seule une amende administrative dont le montant est déterminé en fonction de la capacité économique réelle ou matérielle de son destinataire, et donc imposée par l'autorité de contrôle en se fondant, en ce qui concerne le montant de celle-ci, sur la notion d'unité économique au sens de la jurisprudence citée au point 56 du présent arrêt, est susceptible de réunir les trois conditions énoncées à l'article 83, paragraphe 1, du RGPD, à savoir d'être à la fois effective, proportionnée et dissuasive. Dès lors, lorsqu'une autorité de contrôle décide, au titre des pouvoirs qu'elle détient en vertu de l'article 58, paragraphe 2, du RGPD, d'imposer à un responsable du traitement, qui est ou fait partie d'une entreprise, au sens des articles 101 et 102 TFUE, une amende administrative en application de l'article 83 dudit règlement, cette autorité est tenue de se fonder, en vertu de cette dernière disposition, lue à la lumière du considérant 150 du même règlement, lors du calcul des amendes administratives pour les violations visées aux paragraphes 4 à 6 de cet article 83, sur la notion d'entreprise , au sens de ces articles 101 et 102 TFUE (paragraphes 55 à 59).

147. Cette position a été confirmée par la Cour dans son arrêt du 13 février 2025 (CJUE, cinquième chambre, C-383/23, Ilva A/S).

148. Enfin, le deuxième alinéa de l'article 22 de la loi Informatique et Libertés dispose que la formation restreinte peut rendre publique les mesures qu'elle prend . A.

Sur le prononcé d'une amende administrative et son montant 149. La rapporteure demande à la formation restreinte de prononcer à l'encontre de l'HOPITAL PRIVE DE LA LOIRE une amende administrative au regard des manquements constitués aux articles 32 et 34 du RGPD.

150. En défense, l'hôpital estime le montant de l'amende proposé par la rapporteure disproportionné au regard de sa situation financière et de celle du groupe RAMSAY SANTE. Il rappelle les difficultés rencontrées et met en avant l'augmentation de ses charges de fonctionnement, ainsi que les coûts importants qu'il a d'ores et déjà été contraint de supporter du fait de la violation de données, notamment pour l'intervention d'un cabinet de cybersécurité ainsi que pour la communication aux personnes concernées. Il considère que la formation restreinte devrait tenir compte, conformément à l'article 83, paragraphe 2, du RGPD, de plusieurs circonstances atténuantes telles que la coopération avec l'autorité de contrôle, les mesures prises pour atténuer le dommage, le caractère non délibéré des manquements relevés, liés aux contraintes techniques et organisationnelles du logiciel historique et non d'une volonté de contourner les règles du RGPD, ainsi que le nombre de personnes réellement exposées à un risque, et l'absence de dommage direct porté à la connaissance de la Commission.

151. L'hôpital indique également que le prononcé d'une amende administrative diminuerait d'autant sa capacité à mettre en place les mesures de sécurité que la CNIL préconise et sollicite, à titre principal, l'absence d'amende, et à titre subsidiaire, la réduction significative du montant proposé par la rapporteure. 1.

Sur le prononcé de l'amende 152. La formation restreinte rappelle que, pour évaluer l'opportunité de prononcer une amende, elle doit tenir compte des critères précisés à l'article 83 du RGPD tels que la nature, la gravité et la durée de la violation, la portée ou la finalité du traitement concerné, le nombre de personnes concernées, les mesures prises par le responsable du traitement pour atténuer le dommage subi par les personnes concernées, le fait que la violation a été commise par négligence, le degré de coopération avec l'autorité de contrôle, les catégories de données concernées et le niveau de dommage subi par les personnes.

153. En premier lieu, la formation restreinte considère qu'il y a lieu de faire application du critère prévu à l'alinéa a) de l'article 83, paragraphe 2, du RGPD, relatif à la gravité du manquement compte tenu de la nature, de la portée ou de la finalité du traitement, ainsi que du nombre de personnes affectées.

154. S'agissant des manquements relatifs à la sécurité des données, la formation restreinte rappelle qu'ils ont concerné un nombre important de personnes, à savoir 524 867 patients de l'hôpital, ainsi que 202 246 personnes désignées par ces derniers comme tiers de confiance.

155. Elle considère que les carences de sécurité importantes qui ont été relevées ont permis ou a minima facilité la survenance de la violation, l'attaquant ayant pu accéder aisément au DPI de l'hôpital et extraire durant plusieurs jours un volume de données conséquent sans être repéré.

156. Elle estime que le contexte de recrudescence de cyberattaques exige une attention particulière des responsables du traitement pour assurer la sécurité des données qu'ils traitent. Elle rappelle à cet égard que la CNIL a enregistré en 2025 6 167 notifications de violations de données, le plus haut niveau jamais atteint, qui ont concerné en particulier les secteurs de la santé, de l'administration publique et des activités financières. Elle souligne ainsi que la nature du traitement, en l'occurrence le dossier patient informatisé de l'hôpital, qui centralise à la fois des données administratives permettant d'identifier et de localiser très précisément des personnes, et des données de santé, qui sont des catégories particulières de données à caractère personnel au sens de l'article 9, paragraphe 1, du RGPD, aurait dû conduire l'hôpital à faire preuve d'une vigilance toute particulière lors de la mise en œuvre des mesures devant permettre d'assurer efficacement sa sécurité et sa confidentialité, ce qui n'a pas été le cas.

157. S'agissant du manquement relatif à l'obligation de communication à la personne concernée d'une violation de données à caractère personnel, la formation restreinte rappelle que l'hôpital a omis de prévenir un nombre important de personnes, en l'occurrence 202 246 personnes désignées par des patients de l'hôpital comme tiers de confiance, qui n'ont à ce jour reçu aucune information concernant la nature de l'attaque et ses conséquences probables ni les mesures permettant d'y remédier et de se prémunir d'éventuelles utilisations malveillantes de leurs données à caractère personnel.

158. La formation restreinte considère que cette omission est particulièrement dommageable dès lors que le volume d'informations récupéré par l'attaquant, concernant tant ces personnes que les patients qui les ont désignées comme tiers de confiance, permet des formes sophistiquées d'hameçonnage, voire des usurpations d'identité, notamment pour tenter d'effectuer des formalités administratives au nom d'un patient mineur, majeur protégé ou encore décédé.

159. Il résulte de ce qui précède que les manquements caractérisés à l'égard de l'hôpital sont graves.

160. En deuxième lieu, la formation restreinte estime qu'il convient de tenir compte du critère prévu aux alinéas b) et d) de l'article 83, paragraphe 2, du RGPD, relatifs au fait que la violation ait été commise délibérément ou par négligence, et au degré de responsabilité du responsable de traitement compte tenu des mesures techniques et organisationnelles qu'il a ou non mises en œuvre en vertu des articles 25 et 32 du RGPD.

161. La formation restreinte relève que les mesures de sécurité qui auraient permis d'empêcher ou de limiter la violation sont bien identifiées par l'état de l'art, et que l'hôpital disposait des moyens humains, techniques et financiers pour les mettre en œuvre.

162. Elle souligne que les vulnérabilités identifiées à l'issue des opérations de contrôle sont la conséquence de l'absence de mise en œuvre de mesures élémentaires de sécurité, tant sur le plan technique (en s'abstenant de recourir à un moyen d'identification à deux facteurs ou à un VPN pour l'accès à distance au DPI) que sur le plan organisationnel (en s'abstenant de mettre en œuvre un système d'analyse des journaux permettant de détecter des activités anormales et de déclencher des alertes, et en adoptant une politique d'habilitations inadéquate). Combinées entre elles, ces insuffisances ont fragilisé le système d'information de l'hôpital et ont fait peser sur lui un risque important.

163. La formation restreinte relève que l'hôpital était pourtant conscient de la gravité du risque, dès lors que l'AIPD effectuée en 2021 l'avait qualifiée de maximale , en précisant que l'extrême sensibilité des données concernées par le traitement et les potentielles conséquences des violations justifient amplement ce niveau de gravité .

164. Il incombait donc au responsable de traitement de mettre en œuvre les mesures nécessaires afin de sécuriser le traitement à la hauteur de ce risque, ce qu'il a manqué de faire, et qui a contribué à la survenance de la violation de données des mois de juin-juillet 2025, ainsi qu'à son ampleur.

165. Par conséquent, la formation restreinte considère que les manquements en cause témoignent d'une négligence avérée de la part de l'hôpital.

166. En troisième lieu, la formation restreinte considère qu'il convient de faire application du critère prévu à l'alinéa g) de l'article 83, paragraphe 2 du RGPD relatif aux catégories de données à caractère personnel concernées par le manquement.

167. La formation restreinte relève que le DPI de l'hôpital contient, outre des données de nature administrative, des copies de documents officiels, en l'occurrence les copies de rectos de cartes d'identité des patients, qui constituent des données à caractère relativement sensible , ainsi que des données de santé, qui sont quant à elles des catégories particulières de données à caractère personnel au sens de l'article 9, paragraphe 1, du RGPD, faisant l'objet d'une protection renforcée. La formation restreinte considère ainsi que de telles données aurait dû faire l'objet d'une attention particulière du responsable de traitement, pour en assurer la sécurité et la confidentialité.

168. En conséquence, la formation restreinte estime, au vu de l'ensemble de ces éléments et au regard des critères fixés à l'article 83 du RGPD, qu'il y a lieu de prononcer une amende administrative au titre des manquements en cause. 2.

Sur le montant de l'amende 169. Afin de fixer le montant de l'amende devant être prononcée à l'encontre de la société, il convient de tenir compte de la gravité du manquement commis telle qu'elle résulte de ce qui précède, ainsi que des démarches de mise en conformité déployées à la suite des contrôles et au

cours de la procédure de sanction.

170. La formation restreinte relève d'abord qu'en application de l'article 83 du RGPD, une amende administrative pouvant atteindre 20 millions d'euros ou, s'agissant d'une entreprise, 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu, est susceptible d'être prononcée.

171. En premier lieu, la formation restreinte rappelle que, comme cela est détaillé aux paragraphes 143 à 146, pour déterminer le plafond de l'amende encourue, mais également pour s'assurer de son caractère effectif, dissuasif et proportionné, il convient de recourir à la notion d'entreprise en droit de la concurrence, en vertu de la référence directe et explicite opérée à cette notion par le considérant 150 du RGPD ainsi que par les lignes directrices sur l'application et la fixation des amendes administratives aux fins du règlement 2016/679.

172. La formation restreinte relève que dans son arrêt précité du 5 décembre 2023, la CJUE rappelle qu'une entreprise est une unité économique, même si du point de vue juridique cette unité économique est constituée de plusieurs personnes morales. La CJUE précise qu'à l'instar du droit de la concurrence (Cour de Cassation, ch. com., 7 juin 2023, pourvoi n° 22-10.545 ; Autorité de la concurrence, décisions n° 21-D-10 du 3 mai 2021 et n° 21-D-28 du 9 décembre 2021), lorsqu'une filiale est détenue directement ou indirectement à 100 % par sa maison mère, d'une part cette société mère peut exercer une influence déterminante sur le comportement de cette filiale (...) et, d'autre part, il existe une présomption réfragable selon laquelle ladite société mère exerce effectivement une influence déterminante sur le comportement de sa filiale (CJUE, 10 septembre 2009, C-97/08, point 60). Au demeurant, si cette présomption demeure réfragable, de simples affirmations contraires de la société ne sauraient suffire à renverser la charge de la preuve en l'absence de tout justificatif (CJUE, 16 novembre 2000, C-286/98, point 80).

173. Pour déterminer le montant de l'amende envisagée, et qu'il corresponde à la capacité économique réelle de son destinataire, il convient alors, si les deux sociétés peuvent matériellement être regardées comme relevant de la même unité économique, de prendre en compte le chiffre d'affaires de la maison mère afin que l'amende soit effective, proportionnée et dissuasive (CJUE, cinquième chambre, C-383/23, Ilva A/S , points 22 à 29).

174. En l'espèce, la formation restreinte rappelle que la société HOPITAL PRIVE DE LA LOIRE appartient au groupe RAMSAY SANTE, ces deux entités pouvant être regardées comme relevant de la même unité économique au regard des règles précédemment rappelées.

175. S'agissant du montant de l'amende qui doit être proportionnée et dissuasive, au regard des responsabilités et capacités financières de la société et des critères pertinents de l'article 83 du RGPD, la formation restreinte considère qu'il apparait adapté de prononcer à l'encontre de l'HOPITAL PRIVE DE LA LOIRE une amende administrative d'un montant de cinq cent mille euros (500 000 €) au regard des manquements aux articles 32 et 34 du RGPD. B.

Sur le prononcé d'une injonction assortie d'une astreinte 176. La rapporteure demande à la formation restreinte d'enjoindre à l'HOPITAL PRIVE DE LA LOIRE de se mettre en conformité avec les obligations de l'article 32 du RGPD, en redéfinissant sa politique d'habilitations, en justifiant de la mise en place d'un système de journalisation et d'analyse des traces applicatives et en prenant les mesures techniques visant à n'ouvrir l'accès de l'éditeur du logiciel [...] au DPI que sur autorisation préalable de l'hôpital. Elle propose d'assortir cette injonction d'une astreinte, liquidable à l'issue d'un délai de quinze mois à compter de la notification de la décision.

177. En défense, l'hôpital ne conteste pas l'importance de l'ensemble des mesures prescrites, mais souligne les actions correctives déjà mises en œuvre, à savoir la sécurisation des accès à distance, la gestion améliorée des cartes nationales d'identité des patients, et des travaux sur l'analyse des fichiers de trace.

178. S'agissant des mesures faisant l'objet de l'injonction, il indique qu'elles impliquent une restructuration significative de son système d'information, d'ores et déjà prévue dans le calendrier des différents programmes nationaux de sécurité. Il sollicite, s'agissant des mesures relatives aux habilitations d'accès au DPI, un délai de quinze mois compatible avec le calendrier du programme HospiConnect. Il sollicite également que le montant de l'astreinte proposé par la rapporteure soit réduit.

179. La formation restreinte constate la mise en conformité opérée par l'hôpital en cours de procédure concernant la sécurisation de l'accès à distance au DPI. Elle considère en revanche nécessaire d'enjoindre à l'hôpital de poursuivre sa mise en conformité avec les autres dispositions de l'article 32 du RGPD, en mettant à jour sa politique d'habilitations, en adoptant les mesures nécessaires à la mise en place d'un système de journalisation et d'analyse proactive en temps réel ou à court terme des journaux produits par le système d'information, et en prenant des mesures techniques visant à empêcher l'accès permanent de l'éditeur du logiciel [...] au DPI, et à faire en sorte que tout accès soit systématiquement précédé de l'autorisation de l'hôpital. C.

Sur la publicité de la sanction 180. Le rapporteur demande à la formation restreinte de rendre publique sa décision, et que celle-ci n'identifie plus nommément l'hôpital à l'expiration d'un délai de deux ans à compter de sa publication.

181. L'hôpital s'oppose à cette publication, dont il estime qu'elle lui causerait un préjudice réputationnel majeur et disproportionné, de nature à affecter la confiance des patients et des praticiens. A titre subsidiaire, il sollicite qu'en cas de publication, l'anonymisation intervienne dans un délai réduit, de quelques semaines, ou à tout le moins inférieur aux deux ans proposés par le rapport.

182. La formation restreinte considère qu'une telle mesure de publicité se justifie au regard de la gravité avérée des manquements en cause et du nombre de personnes concernées, lesquelles doivent être informées.

183. Elle estime en outre que cette mesure apparait proportionnée dès lors que la décision n'identifiera plus nommément la société à l'issue d'un délai de deux ans à compter de sa publication.

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

- prononcer à l'encontre de la société HOPITAL PRIVE DE LA LOIRE une amende administrative d'un montant de cinq cent mille euros (500 000 €) au regard des manquements constitués aux articles 32 et 34 du RGPD ;

- prononcer à l'encontre de la société HOPITAL PRIVE DE LA LOIRE une injonction de mettre en conformité le traitement avec les dispositions de l'article 32 du RGPD, et en particulier : o de mettre en place un système de journalisation et d'analyse proactive en temps réel ou à très court terme des journaux produits par le système d'information afin de détecter le comportement anormal d'utilisateurs et de déclencher des alertes et réponses appropriées, dans un délai de trois mois, sous astreinte de mille euros (1 000 €) par jour de retard ; o de mettre à jour de sa politique d'habilitations, en tenant notamment compte des dispositions des articles L. 1110-4 et L. 1110-12 du code de la santé publique relatives à la notion d'équipe de soins , afin que seules les personnes ayant besoin d'en connaître aient accès, par défaut, aux données (et en prévoyant, pour les cas d'urgence, un mécanisme de type bris de glace), dans un délai de quinze mois, sous astreinte de mille euros (1 000 €) par jour de retard ; o de mettre en place de mesures techniques visant à n'ouvrir l'accès de l'éditeur du logiciel Expert Santé au DPI que sur autorisation préalable de l'hôpital, dans un délai de trois mois, sous astreinte de mille euros (1 000 €) par jour de retard ; les justificatifs de la mise en conformité devant être adressés à la formation restreinte dans les délais précités ;

- rendre publique, sur le site web de la CNIL et sur le site web de Légifrance, sa délibération, qui ne permettra plus d'identifier nommément la société à l'issue d'une durée de deux ans à compter de sa publication. Le président 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. Philippe-Pierre CABOURDIN