Délibération SAN-2024-013 du 5 septembre 2024

Commission Nationale de l'Informatique et des Libertés

Nature de la délibération : Sanction
Etat juridique : En vigueur

Date de publication sur Légifrance : Jeudi 12 septembre 2024

Délibération de la formation restreinte n°SAN-2024-013 du 5 septembre 2024 concernant la société CEGEDIM SANTÉ

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 Isabelle LATOURNARIE-WILLEMS et Laurence FRANCESCHINI et M. Alain DRU, membres ;

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

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

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° 2020-085C du 12 mai 2020 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 CEGEDIM LOGICIEL MEDICAUX FRANCE, par ses filiales ou pour son compte, en tout lieu susceptible d'être concerné par leur mise en œuvre ;

Vu la décision de la présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur devant la formation restreinte, en date du 2 mars 2023 ;

Vu le rapport de Monsieur François PELLEGRINI, commissaire rapporteur, notifié à la société CEGEDIM SANTÉ le 12 octobre 2023 ;

Vu les observations écrites versées par la société les 17 novembre 2023, 8 janvier et 21 mai 2024 ;

Vu les réponses du rapporteur à ces observations, notifiées à la société les 8 décembre 2023 et 15 mars 2024 ;

Vu l'arrivée à échéance du mandat de commissaire de Monsieur François PELLEGRINI le 1erfévrier 2024 ;

Vu la décision de la présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un nouveau rapporteur, Monsieur Claude CASTELLUCCIA, devant la formation restreinte, en date du 31 janvier 2024 ;

Vu la clôture de l'instruction, notifiée à la société le 28 mai 2024 ;

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

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte du 13 juin 2024 :

- Monsieur Claude CASTELLUCCIA, commissaire, entendu en son rapport ;

En qualité de représentants de la société CEGEDIM SANTÉ :

- […] ;

La société CEGEDIM SANTÉ ayant eu la parole en dernier ;

La formation restreinte a adopté la décision suivante :

I. Faits et procédure

1. La société CEGEDIM LOGICIELS MEDICAUX FRANCE, dont le siège social est situé au 137, rue d'Aguesseau à Boulogne-Billancourt (92100), est une société par actions simplifiée à associé unique. En 2020 et 2021, elle a réalisé un chiffre d'affaires de […] et de […] et un résultat net de […] et de […].

2. L'associé unique de la société CEGEDIM LOGICIELS MEDICAUX FRANCE est la société CEGEDIM SANTÉ (ci-après la société), société par actions simplifiée, dont le siège social est sis au 137, rue d'Aguesseau, 92100 Boulogne-Billancourt.

3. En sa qualité d'associé unique, la société CEGEDIM SANTÉ a décidé la dissolution anticipée sans liquidation de la société CEGEDIM LOGICIELS MEDICAUX FRANCE à compter du 22 novembre 2021. La société CEGEDIM SANTÉ a repris l'intégralité des activités de la société CEGEDIM LOGICIELS MEDICAUX FRANCE, ainsi que les traitements des données à caractère personnel qu'elle réalisait.

4. La société CEGEDIM SANTÉ fait partie du groupe CEGEDIM, spécialisé dans la gestion des flux numériques de l'écosystème santé entre professionnels et dans la conception de logiciels métier, destinés notamment aux professionnels de santé. En 2022, le chiffre d'affaires du groupe CEGEDIM s'est élevé à […] et son résultat net à […].

5. L'activité de la société CEGEDIM SANTÉ consiste à éditer et vendre des logiciels de gestion aux médecins de ville exerçant en cabinets et en centres de santé. Environ 25 000 cabinets médicaux et 500 centres de santé utilisent les logiciels proposés par la société. Celle-ci édite notamment le logiciel CROSSWAY, qui permet aux médecins de gérer leur agenda, les dossiers de leurs patients et leurs prescriptions.

6. La société propose à un panel de médecins de ville utilisant ce logiciel, éligibles en fonction de critères géographiques, d'âges et de spécialités, d'adhérer à un observatoire en vue de collecter des données issues des dossiers des patients. En cas d'adhésion à l'observatoire , les données contenues dans les logiciels des médecins sont extraites dans le flux CROSSWAY afin d'être ensuite utilisées dans le cadre d'études et de statistiques dans le domaine de la santé réalisées par les clients de la société CEGEDIM SANTÉ, dont les sociétés […] et […]. À titre d'exemples, les clients de la société CEGEDIM SANTÉ réalisent des études sur la prise en charge des patients en fonction de leurs pathologies, sur les disparités démographiques, régionales et les profils de prise en charge des médecins et la mesure de la consommation de soins. En 2021, environ […] médecins avaient adhéré à cet observatoire .

7. En contrepartie, les médecins du panel bénéficient d'une remise sur la licence d'utilisation du logiciel CROSSWAY et la société leur donne accès aux études statistiques réalisées par la […] , ainsi qu'à des tableaux de bord personnalisés.

8. Par décision n° 2020-085C du 12 mai 2020, la présidente de la Commission nationale de l'informatique et des libertés (ci-après la Commission ou la CNIL) a chargé le secrétaire général de procéder ou de faire procéder à une mission de vérification des traitements mis en œuvre par la société CEGEDIM LOGICIEL MEDICAUX FRANCE, par ses filiales ou pour son compte, en tout lieu susceptible d'être concerné par leur mise en œuvre.

9. Le 30 mars 2021, une délégation de la CNIL a procédé à un contrôle dans les locaux de la société, afin de vérifier le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (ci-après la loi Informatique et Libertés ou loi du 6 janvier 1978 modifiée) et du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données à caractère personnel et à la libre circulation de ces données (ci-après le Règlement ou RGPD).

10. Les 12 avril 2021 et 16 février 2023, la société a fourni des éléments complémentaires sollicités par la délégation lors du contrôle sur place.

11. Aux fins d'instruction de ces éléments, la présidente de la Commission a, le 2 mars 2023, désigné Monsieur François PELLEGRINI en qualité de rapporteur sur le fondement de l'article 39 du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi Informatique et Libertés.

12. Le 12 octobre 2023, à l'issue de son instruction, le rapporteur a fait notifier à la société un rapport détaillant les manquements à l'article 5, paragraphe 1, a) du RGPD et à l'article 66 de la loi Informatique et Libertés qu'il estimait constitués en l'espèce. Ce rapport proposait à la formation restreinte de prononcer une amende administrative à

l'encontre de la société et une injonction assortie d'une astreinte de se mettre en conformité avec les manquements constatés. Il proposait également que cette décision soit rendue publique.

13. Le 17 novembre 2023, la société a produit des observations en réponse au rapport de sanction.

14. Le rapporteur a répondu aux observations de la société le 8 décembre 2023.

15. Le 8 janvier 2024, la société a produit ses deuxièmes observations en réponse.

16. Le mandat de commissaire de Monsieur François PELLEGRINI arrivant à son terme le 1er février 2024, la présidente de la CNIL a désigné Monsieur Claude CASTELLUCCIA en qualité de rapporteur le 31 janvier 2024, en application de l'article 40 I alinéa 5 du décret n° 2019-536 du 29 mai 2019.

17. Le 15 mars 2024, le rapporteur a produit une réponse aux deuxièmes observations de la société.

18. Le 21 mai 2024, la société a produit ses troisièmes observations.

19. Par courrier du 27 mai 2024, le rapporteur a, en application du III de l'article 40 du décret n° 2019-536 précité, informé la société et le président de la formation restreinte que l'instruction était close.

20. Par courrier du 27 mai 2024, la société a été informée que le dossier était inscrit à l'ordre du jour de la formation restreinte du 13 juin 2024.

21. Le 12 juin 2024, la société a, par l'intermédiaire de son conseil, sollicité le report de la clôture de l'instruction jusqu'à la tenue de la séance de la formation restreinte prévue le lendemain, afin de pouvoir verser une pièce complémentaire, à savoir la copie d'un courrier adressé par la société CEGEDIM LOGICIELS MEDICAUX à la CNIL le 25 avril 2013. Le président de la formation restreinte a fait droit à cette demande.

22. Le rapporteur et la société ont présenté des observations orales lors de la séance de la formation restreinte.

II. Motifs de la décision

A. Sur le grief tiré de la méconnaissance des droits de la défense et du droit à un procès équitable

23. La société soutient qu'il a été porté atteinte à ses droits de la défense dans la mesure où, par courrier du 21 décembre 2023, le président de la formation restreinte lui a refusé l'extension de délai sollicité pour produire ses deuxièmes observations, en méconnaissance du droit à un procès équitable selon elle. Elle précise que, pour pouvoir répondre aux nouveaux arguments avancés par le rapporteur concernant plus particulièrement l'analyse du risque de réidentification pour lequel celle-ci estime que des analyses complémentaires sont nécessaires, la société a dû faire appel à un expert, qui n'était en mesure de rendre ses conclusions que pour la mi-janvier 2024, alors que son délai pour répondre expirait le 8 janvier 2024.

24. La société soutient par ailleurs que des éléments de preuve essentiels qu'elle a invoqués en défense pour démontrer le caractère anonyme des données du flux CROSSWAY n'ont pas été repris par le rapporteur, de sorte qu'elle s'interroge sur la prise en compte effective de ses arguments et donc sur le respect de ses droits de la défense et sur la garantie d'un procès équitable.

25. En premier lieu, la formation restreinte relève que les délais qui ont été appliqués dans le cadre de la procédure contradictoire sont ceux définis par l'article 40 I du décret n° 2019-536 précité. Elle note que la société a en outre bénéficié d'un délai de cinq jours supplémentaires pour produire ses premières observations en défense, conformément à sa demande formulée auprès du président de la formation restreinte.

26. En deuxième lieu, la formation restreinte souligne que le rapport de sanction a été notifié à la société dès le 12 octobre 2023. Rien ne faisait donc obstacle à ce qu'elle mandate un expert dès cette date puisque, dès le rapport de sanction, le rapporteur considérait que les données que la société traite ne sont pas anonymes mais pseudonymes. L'analyse et la position du rapporteur sur ce point ont été constantes dans le cadre de la procédure de sanction et exposées dès le rapport de sanction. La société aurait donc pu solliciter un expert bien avant la réception de la réponse du rapporteur à ses premières observations en défense.

27. En troisième lieu, la formation restreinte relève que la société a pu produire les conclusions de l'expertise utiles à sa défense qu'elle souhaitait produire, puisque le rapporteur n'a pas clos l'instruction à l'issue des deuxièmes observations en défense de la société. Il a en effet décidé d'adresser une deuxième réponse aux observations de la société, laquelle a disposé d'un délai de deux mois et sept jours pour produire ses troisièmes observations en réponse.

28. En dernier lieu, si la société estime que le rapporteur n'a pas suffisamment pris en compte les arguments qu'elle avance dans ses différents écrits et a commis différentes erreurs d'appréciation, la formation restreinte rappelle que l'ensemble des écritures et pièces produites à la fois par la société et par le rapporteur ont bien été portées à sa connaissance, et qu'elle dispose ainsi des éléments nécessaires afin de se prononcer sur le traitement en cause. La formation restreinte relève également que la société a pu présenter ses observations en défense dans ses trois jeux d'écriture, plusieurs tours de contradictoire ayant eu lieu dans le cadre de cette procédure, ainsi qu'oralement lors de la séance de formation restreinte du 13 juin 2024.

29. La formation restreinte considère dès lors que le grief tiré de la méconnaissance de ses droits de la défense et du droit à un procès équitable doit être écarté.

B. Sur le traitement en cause et la responsabilité de traitement

30. Au moment du contrôle effectué par la CNIL et jusqu'en 2022, la société collectait un certain nombre de données auprès des médecins panélistes ayant adhéré à son observatoire . Ces données étaient relatives à la fois au dossier administratif des patients (numéros de patient, année de naissance, sexe, catégorie socio-professionnelle, code de la région, date de la consultation), au dossier médical (allergies, antécédents du patient, antécédents familiaux, taille, poids, pouls, tension, diagnostics du jour etc.), aux prescriptions pharmaceutiques (médicament, posologie, durée, etc.) et aux autres prescriptions (arrêt de travail, vaccins, résultats d'examens biologiques, etc.).

31. Toutes ces données sont chiffrées et reliées à un identifiant unique pour chaque patient, qui ne repose sur aucun trait d'identité du patient. Les données des patients sont extraites périodiquement du flux CROSSWAY pour constituer un fichier sur le poste du médecin panéliste. Lors de la génération de ce fichier, les numéros patients du flux sont rechiffrés. Le fichier est ensuite acheminé par canal chiffré HTTPS vers le serveur hébergeant la base de données qui agrège et stocke transitoirement les données. Ainsi, même si chaque patient se voit attribuer des identifiants différents dans le flux CROSSWAY et dans les fichiers transmis par les médecins à la société CEGEDIM SANTÉ, l'ensemble des données concernant un même patient du même médecin est bien toujours associé à ce deuxième identifiant dans le jeu de données communiqué à la société CEGEDIM SANTÉ. En revanche, un même patient se rendant dans un autre cabinet médical se verra attribuer un autre identifiant unique propre à cet autre cabinet. L'identifiant étant lié aux données médicales et administratives d'un même patient, il permet donc le suivi de l'historique du patient pour un seul et même cabinet.

32. Les lignes présentes dans la base de données sont composées des identifiants du patient et du médecin consulté, ainsi que de divers codes. […]. D'après les chiffres communiqués par la société, le nombre de lignes collectées entre le 1er janvier 2021 et le 2 avril 2021 par la société CEGEDIM SANTÉ est de plus de […].

33. Les données sont conservées trois mois à compter de leur réception dans le flux CROSSWAY. Ensuite, elles sont transmises aux clients de la société, dont la société […], qui réalise des études et statistiques dans le domaine de la santé. Bien que les données ne soient conservées que trois mois dans le flux, certaines présentent une profondeur historique plus importante. Par exemple, les données issues du téléservice HRi, qui sera évoqué ci-après, sont automatiquement téléchargées sur une profondeur de douze mois lorsque le médecin les consulte.

34. La société CEGEDIM SANTÉ considère que les données qu'elle traite sont anonymes et ne sont donc plus soumises au régime applicable en matière de protection des données à caractère personnel.

35. Le rapporteur estime quant à lui que la société s'est constituée un entrepôt de données de santé pseudonymisées à partir des données que lui communiquent les médecins panélistes, afin de les mettre à disposition de ses clients – dont certains appartiennent au même groupe – qui réalisent des études et statistiques dans le domaine de la santé. Ainsi, le rapporteur estime que la société CEGEDIM SANTÉ est tenue de se conformer à la règlementation relative à la protection des données à caractère personnel pour traiter lesdites données et, notamment, de disposer d'une autorisation pour ce faire.

36. En défense, la société fait également valoir qu'elle a mis en œuvre, depuis 2022, des nouvelles mesures d'appauvrissement des données au stade de l'extraction, données qui sont depuis lors moins précises. Elle ne collecte par exemple plus les informations des patients dont l'année de naissance est inférieure ou égale à 1920 ou si le patient est âgé de plus de 95 ans, elle ne collecte plus le nombre exact d'enfants des patients (0 si pas d'enfants, 1 si 1 enfant ou plus, et si le patient a moins de 18 ans le nombre d'enfants est systématiquement à 0) ou encore ne collecte plus les informations des patients ayant un sexe indéterminé.

37. La formation restreinte considère qu'il y a lieu d'examiner la nature des données traitées et la qualification du traitement avant de pouvoir déterminer les responsabilités associées à celui-ci.

1) Sur la nature des données traitées dans le flux CROSSWAY

a) Sur le cadre juridique applicable

38. L’article 4, paragraphe 1, du RGPD définit la notion de données à caractère personnel comme toute information se rapportant à une personne physique identifiée ou identifiable […] ; est réputée être une personne physique identifiable une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification […] .

39. L’article 4, paragraphe 15, du RGPD dispose que les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne constituent des données de santé.

40. L’article 4, paragraphe 5, du RGPD définit la pseudonymisation comme le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable .

41. La formation restreinte relève que, contrairement à la notion de pseudonymisation, la notion d’anonymisation n’est pas définie par le RGPD.

42. Le considérant 26 du RGPD dispose que Les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable. Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci. Il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable. Le présent règlement ne s'applique, par conséquent, pas au traitement de telles informations anonymes, y compris à des fins statistiques ou de recherche .

43. Dans son arrêt Breyer rendu sous l’empire de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (CJUE, 2ème chambre, 19 octobre 2016, C-582/14), la Cour de justice de l’Union européenne (ci-après la CJUE) a jugé que le considérant 26 de la directive 95/46 énonce que, pour déterminer si une personne est identifiable, il convient de considérer l’ensemble des moyens susceptibles d’être raisonnablement mis en œuvre soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne (§ 42) et que dans la mesure où ce considérant fait référence aux moyens susceptibles d’être raisonnablement mis en œuvre tant par le responsable du traitement que par une autre personne , le libellé de celui-ci suggère que, pour qu’une donnée puisse être qualifiée de donnée à caractère personnel […], il n’est pas requis que toutes les informations permettant d’identifier la personne concernée doivent se trouver entre les mains d’une seule personne (§ 43).

44. Cette jurisprudence a été confirmée dans l’arrêt OC c/ Commission européenne (CJUE, 6ème chambre, 7 mars 2024, C-479/22). Dans ladite affaire, la CJUE a jugé que la circonstance que des informations supplémentaires sont nécessaires pour identifier la personne concernée n’est pas de nature à exclure que les données en cause puissent être qualifiées de données à caractère personnel (§ 49), tout en prenant en compte le fait que la possibilité de combiner les données en cause avec des informations supplémentaires constitue un moyen susceptible d’être raisonnablement mis en œuvre pour identifier la personne concernée en prenant en considération l’ensemble des facteurs objectifs tels que le coût de l’identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l’évolution de celles-ci (§ 50).

45. La CJUE précise en outre dans cet arrêt qu’ il est inhérent à l’ identification indirecte d’une personne que des informations supplémentaires doivent être combinées avec les données en cause aux fins de l’identification de la personne visée (§ 55) et que la requérante n’était pas tenue d’apporter la preuve qu’elle avait effectivement été identifiée par l’une de ces personnes, puisqu’une telle condition n’est pas prévue à l’article 3, point 1, du règlement 2018/1725, celui-ci se limitant à exiger qu’une personne soit identifiable (§ 61).

46. Enfin, dans l’arrêt IAB Europe c/ Gegevensbeschermingsautoriteit (CJUE, 4ème chambre, 7 mars 2024, C-604/22), la Cour a considéré que L’article 4, point 1, du RGPD doit être interprété en ce sens qu’une chaîne composée d’une combinaison de lettres et de caractères, telle que la TC String [Transparency and Consent String], contenant les préférences d’un utilisateur d’Internet ou d’une application relatives au consentement de cet utilisateur au traitement des données à caractère personnel le concernant par des fournisseurs de sites Internet ou d’applications ainsi que par des

courtiers de telles données et par des plateformes publicitaires, constitue une donnée à caractère personnel au sens de cette disposition dans la mesure où, lorsque celle-ci peut, par des moyens raisonnables, être associée à un identifiant, tels que notamment l'adresse IP de l'appareil dudit utilisateur, elle permet d'identifier la personne concernée. . Elle ajoute que la circonstance que, sans une contribution extérieure, une organisation sectorielle détenant cette chaîne ne peut ni accéder aux données qui sont traitées par ses membres dans le cadre des règles qu'elle a établies ni combiner ladite chaîne avec d'autres éléments ne fait pas obstacle à ce que la même chaîne constitue une donnée à caractère personnel au sens de ladite disposition (§ 51).

47. Enfin, à titre d'éclairage, la formation restreinte relève que, dans son Avis 05/2014 sur les techniques d'anonymisation du 10 avril 2014, le Groupe de travail Article 29 sur la protection des données (ci-après G29), devenu le Comité européen de la protection des données (ci-après CEPD), indique qu'un processus peut notamment être qualifié d'anonymisation lorsqu'il résiste aux trois types de risques suivants :

- l'individualisation, qui correspond à la possibilité d'isoler une partie ou la totalité des enregistrements identifiant un individu dans l'ensemble de données ;

- la corrélation, qui consiste en la capacité de relier entre elles, au moins, deux enregistrements se rapportant à la même personne concernée ou à un groupe de personnes concernées ;

- l'inférence, qui est la possibilité de déduire, avec un degré de probabilité élevé, la valeur d'un attribut à partir des valeurs d'un ensemble d'autres attributs.

48. À défaut de résister aux trois types de risques mentionnés ci-dessus, les données ne seront pas nécessairement qualifiées de pseudonymes . Elles pourront être qualifiées d'anonymes dans l'hypothèse où le responsable de traitement est en mesure de démontrer que la réidentification n'est pas possible par des moyens raisonnables , c'est-à-dire que les risques de réidentification sont négligeables.

49. Le rapporteur fait valoir, à la lumière des différents éléments issus de la jurisprudence et de la doctrine, qu'il ne fait pas doute que le cadre juridique applicable permet d'apprécier le caractère anonyme ou pseudonyme des données traitées et de déterminer que, de manière constante, le suivi de personnes dans la durée, à l'aide d'un identifiant unique, permet d'isoler un individu dans un jeu de données et augmente donc le risque de levée du pseudonymat.

50. La société considère au contraire que le cadre légal, jurisprudentiel et doctrinal autour de la question de l'anonymisation de données est source d'insécurité juridique pour les opérateurs. Elle souligne le manque de clarté de ce cadre et l'absence de référentiels, de méthodologies ou de prescriptions techniques permettant de démontrer le caractère anonyme d'un jeu de données. Elle soutient que les publications, notamment de la CNIL, du G29 et du CEPD, ne permettent pas d'assurer le respect du principe de prévisibilité du droit découlant de l'exigence constitutionnelle de sécurité juridique en droit français en ce qu'elles ne présentent pas de prescriptions, notamment techniques, suffisamment claires que ce soit pour permettre aux opérateurs d'assurer une confiance raisonnable dans le résultat des procédés d'anonymisation utilisés ou pour assurer la recevabilité de la preuve de l'anonymisation vis-à-vis de la CNIL. La société fait valoir différents arguments afin d'appuyer sa position.

51. Premièrement, la société fait état d'une décision rendue par le juge du tribunal de Milan (tribunal de Milan, ordonnance du 4 décembre 2023), dans le cadre d'un contentieux opposant l'autorité de protection des données italienne […] -, qui poursuit une activité similaire à celle de la société CEGEDIM SANTÉ au titre de l'observatoire . Selon la société, le juge a considéré qu'en l'état des éléments, l'autorité italienne n'avait pas démontré que les données n'étaient pas anonymes et qu'une expertise indépendante devait être conduite pour vérifier le caractère anonyme des données, les possibilités de réidentification des personnes, ainsi que le risque concret de cette réidentification en tenant compte du temps et des coûts nécessaires.

52. Deuxièmement, la société fait valoir qu'elle est fondée à se baser sur l'acceptation probabiliste de la notion de donnée à caractère personnel, estimant que l'analyse du risque d'identification ne doit pas nécessairement tendre à réduire ce risque à zéro, mais plutôt à réduire ce risque à un niveau acceptable au regard de la sensibilité des données, du contexte et des finalités du traitement. Elle cite à l'appui un document commun de l'autorité espagnole de protection des données et du CEPD publié en juin 2021, ainsi qu'un article publié et corédigé par le rapporteur, Monsieur CASTELLUCCIA, en 2020.

53. Troisièmement, elle fait valoir que le fait qu'un jeu de données puisse être relié à un identifiant n'exclut pas que ces données puissent être anonymes, à l'instar des données contenues dans la base OpenDamir du SNIIRAM. La société estime que si les données de l'OpenDamir, plus précises à de nombreux égards que celles traitées par CEGEDIM SANTÉ, ont pu être considérées comme anonymes, celles doivent également l'être.

54. Enfin, la société soutient que même en cas d'identification d'un code patient associé aux informations connues sur l'individu recherché dans le flux CROSSWAY, cela ne conduit pas nécessairement à la réidentification. En effet, elle soutient qu'il n'existe qu'une certaine probabilité que les informations retrouvées dans la base soient celles de la personne

recherchée. Elle estime que de multiples incertitudes mettent en échec la possibilité de réidentification , par exemple parce qu'un individu peut partager les caractéristiques connues avec d'autres individus ou encore parce qu'il n'est pas possible de savoir si l'individu recherché est présent ou non dans la base. La société cite à l'appui un extrait d'une publication de la Direction de la recherche, des études de l'évaluation et des statistiques (DREES).

55. À titre liminaire, la formation restreinte rappelle que, si la CNIL dispose de pouvoirs de publication de lignes directrices, recommandations ou référentiels destinés à faciliter la mise en conformité des traitements de données à caractère personnel avec les textes relatifs à la protection des données à caractère personnel (en application de l'article 8, paragraphe 2, b) de la loi Informatique et Libertés), les règles juridiques sont fixées par les législateurs français et européen, et interprétées par les juridictions compétentes. Ainsi, quand bien même la CNIL n'a pas publié de référentiels ou de lignes directrices spécifiques aux notions de pseudonymisation et d'anonymisation, la formation restreinte relève que le CEPD a publié des lignes directrices qui demeurent pertinentes. La formation restreinte souligne que les écritures produites tant par le rapporteur que par la société révèlent que ces notions font l'objet de nombreuses publications, tant sur le plan jurisprudentiel que doctrinal. L'absence de référentiels, lignes directrices ou recommandations de la CNIL ne saurait donc être suffisante pour considérer que le cadre juridique applicable n'est pas clair.

56. S'agissant ensuite de la décision rendue par le tribunal de Milan, la formation restreinte observe que le juge a décidé de suspendre l'efficacité exécutive de la décision de l'autorité de protection des données italienne uniquement concernant les sanctions accessoires de publication sur le site de la société et de transmission aux ordres et fédérations concernés, dans l'attente qu'une expertise indépendante soit menée, afin de déterminer si les données traités par la filiale italienne de CEGEDIM SANTÉ sont pseudonymisées ou anonymisées.

57. La formation restreinte constate que le juge ne suspend en revanche pas l'amende et l'injonction prononcées. Il n'affirme pas non plus que les données traitées sont anonymes. La formation restreinte souligne à cet égard que l'autorité italienne de protection des données a estimé dans sa décision que les données traitées sont des données à caractère personnel, notamment puisqu'un identifiant unique est attribué à chaque patient.

58. S'agissant de la base OpenDamir évoquée par la société, la formation restreinte observe que les deux traitements ne sont pas comparables dans la mesure où dans OpenDamir, chaque ligne correspond à un remboursement de l'assurance maladie et non à un patient. Un fichier est édité chaque mois et il est impossible de suivre le parcours médical d'un même patient dans le temps via OpenDamir. Au contraire, dans le traitement en cause, la société CEGEDIM SANTÉ est en mesure d'identifier que plusieurs fichiers transmis successivement par un même médecin concernent un même patient.

59. En outre, s'agissant de l'étude de la DREES citée par la société, la formation restreinte relève qu'elle précise également qu' une accumulation de ressemblances avec une personne connue pourrait, au fil de l'addition des millésimes diffusés, au fur et à mesure de l'enrichissement annuel de la base, conduire à une probabilité d'identification proche de l'unité , ce qui correspond à la façon dont le traitement mis en œuvre par CEGEDIM SANTÉ est construit puisqu'il est possible de retracer le parcours de soins précis d'un patient d'un même médecin dans le temps et que la société dispose d'un large volume de données. Cette même étude de la DREES indique clairement que le remplacement de l'identifiant initial d'une personne par un autre identifiant arbitraire correspond à une pseudonymisation et non à une anonymisation. Ainsi, la formation restreinte considère que la mobilisation de cette étude de la DREES par la société n'est pas pertinente en l'espèce.

60. Enfin, la formation restreinte relève qu'il n'y a pas débat, ni dans la jurisprudence, ni dans la doctrine, sur le fait que l'attribution d'un code ou identifiant unique à des personnes afin de permettre leur suivi permet leur individualisation dans le jeu de données. En outre, il est clairement établi que pour évaluer le risque que soit levé le pseudonymat, il convient d'intégrer la possibilité de combiner un premier jeu de données avec d'autres données, lesquelles peuvent être détenues par des tiers. Au titre de ces autres données figurent par exemple les données de géolocalisation.

b) Sur la nature des données traitées

61. S'agissant des données de patients, le rapporteur relève qu'il ressort des pièces du dossier que chaque patient se voit attribuer un identifiant unique pour un même médecin au sein du flux CROSSWAY. Ce numéro, qui ne repose sur aucun trait d'identité, est lié aux données médicales et administratives d'un même patient et permet donc le suivi de l'historique du patient pour un même médecin. Par conséquent, le rapporteur considère que, grâce à l'identifiant du patient qui lui est communiqué, la société CEGEDIM SANTÉ est en mesure d'identifier que plusieurs fichiers transmis successivement par un même médecin concernent un même patient au sein de son observatoire .

62. Le rapporteur en conclut que :

- d'une part, ce procédé, consistant à remplacer les données directement identifiantes par des données indirectement identifiantes, à savoir un identifiant unique pour le patient concerné d'un même médecin, correspond parfaitement à la définition de la pseudonymisation, et permet d'avoir un suivi longitudinal du patient ;

- d'autre part, dès lors qu'il est possible d'isoler ainsi un individu dans le jeu de données et d'accroître au cours du temps l'ensemble des données qui le concernent, les données des patients sont suffisamment riches pour permettre une levée du pseudonymat par des moyens raisonnables.

63. Dans le cadre des échanges contradictoires avec la société, le rapporteur a produit à l'appui de son analyse une démonstration dans laquelle il parvient à retracer avec précision le parcours de soins d'un enfant de 12 ans en ALD à partir de quelques lignes de données uniquement transmises par la société dans le cadre de la procédure de contrôle.

64. S'agissant des données des médecins, le rapporteur relève que la société génère un numéro de panel à partir du numéro de client du médecin et que ce numéro apparaît dans les fichiers générés par les médecins panélistes, transmis à CEGEDIM SANTÉ. Le rapporteur relève par ailleurs que la société dispose d'une table de correspondance entre le numéro de panel et l'identité du médecin et en conclut que la détention de cette table rend encore plus précises les données détenues par la société. Ainsi, le rapporteur considère que la société est en mesure d'identifier, parmi l'ensemble des panélistes, qu'un même médecin lui communique des fichiers et que dès lors, il s'agit de données pseudonymisées.

65. En défense, la société considère que les données sont anonymes. Elle considère que la démonstration du rapporteur est théorique et entièrement focalisée sur les possibilités d'individualisation des personnes à partir des données du flux CROSSWAY, le rapporteur ne cherchant à aucun moment à évaluer de manière précise et objective les risques réels et résiduels de réidentification des patients selon des moyens raisonnables susceptibles d'être utilisés par la société, dont notamment les éléments de contexte précis.

66. Or, la société soutient que le caractère identifiable d'une personne, permettant de considérer que des données constituent des données à caractère personnel, ne peut être affirmé par postulat, mais doit être validé par une analyse in concreto des moyens raisonnables permettant l'identification. Elle estime qu'il ressort des décisions Breyer et OC c/ Commission européenne précitées que ces moyens raisonnables doivent correspondre à des moyens légaux et mobilisables en pratique, prenant notamment en compte des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement. Elle ajoute qu'au-delà de l'analyse des éléments de contexte précis et de la quantification de l'éventualité de leur réalisation au regard des facteurs objectifs (temps, coût, main d'œuvre, technologies disponibles), il convient également de prendre en compte les motivations des personnes pouvant procéder à la réidentification.

67. À l'appui de ses déclarations, la société produit une évaluation externe réalisée par la société […], mandatée par la société […], relative aux données de la base […] alimentée par le flux CROSSWAY. Ladite évaluation conclut à la nature anonyme des données.

68. Enfin, s'agissant de la table de correspondance détenue par la société, celle-ci soutient que la table recensant les codes et l'identité des médecins participant à l'observatoire ne peut être considérée comme un moyen raisonnable susceptible de pouvoir être utilisé pour aider à la réidentification des patients. En effet, la société fait valoir que la table de correspondance est gérée par une équipe dédiée et distincte de celle en charge d'opérer le flux CROSSWAY, sur un poste informatique isolé, avec un cloisonnement total des informations et une parfaite étanchéité des rôles et responsabilités entre ces deux équipes.

69. En premier lieu, la formation restreinte relève que le caractère pseudonyme ou anonyme des données présente un enjeu particulièrement important pour les personnes concernées puisque, si les données ne sont pas des données à caractère personnel, la règlementation en matière de protection des données ne leur est pas applicable et donc l'utilisation qui peut en être faite est totalement libre. En particulier, une base de données anonymes n'est pas soumise aux obligations de sécurisation fixées par l'article 32 du RGPD et peut être librement communiquée ou publiée. L'organisme qui opère une telle base n'est tenu à aucune obligation d'information.

70. En l'espèce, s'agissant des données des patients, la formation restreinte relève que la société CEGEDIM SANTÉ, au moment du contrôle effectué par la CNIL et jusqu'en 2022, collectait de très nombreuses données auprès des médecins panélistes relatives à la fois au dossier administratif des patients, au dossier médical, aux prescriptions pharmaceutiques et aux autres prescriptions. La formation restreinte relève que la société a indiqué, depuis 2022, ne plus collecter d'informations relatives à la catégorie socio-professionnelle, à la situation familiale et au nombre d'enfants. Le code de la région a également été supprimé et la société a indiqué avoir appauvri les mesures de taille et de poids.

71. La formation restreinte relève que, même si chaque patient se voit attribuer des identifiants différents dans le flux CROSSWAY et dans les fichiers transmis par les médecins à la société CEGEDIM SANTÉ, l'ensemble des données concernant un même patient d'un même médecin reste associé à ce deuxième identifiant dans le jeu de données communiqué à la société CEGEDIM SANTÉ. Dès lors, grâce à l'identifiant du patient qui lui est communiqué, la société CEGEDIM SANTÉ est en mesure de relier à un même identifiant plusieurs fichiers transmis successivement par un même médecin concernant un même patient, ce que la société ne conteste d'ailleurs pas, et de disposer ainsi de son parcours de soins auprès de ce médecin.

72. Ainsi, la formation restreinte relève qu'il est possible d'isoler un individu dans le jeu de données dans la mesure où l'identifiant unique permet de suivre les patients au fil du temps. Dès lors, par nature, le traitement ne résiste pas au risque de l'individualisation tel que décrit dans l'Avis 05/2014 sur les techniques d'anonymisation du 10 avril 2014 précité.

73. S'agissant par ailleurs des données des médecins, la formation restreinte relève que la société CEGEDIM SANTÉ est en mesure d'identifier, parmi l'ensemble des médecins panélistes et grâce à l'identifiant du médecin, qu'un même médecin lui communique des fichiers.

74. En deuxième lieu, la formation restreinte observe que les données recueillies sont particulièrement riches et la profondeur de données importante : d'une part car la société traite de nombreuses données ; d'autre part car, bien que la société ne conserve les données que trois mois dans sa base, elle récupère via le téléservice HRi des données sur une profondeur de douze mois, qui contiennent des informations relatives à l'historique des remboursements de santé effectués par l'assurance maladie pour un patient. Cet ensemble de données particulièrement riche et exhaustif permet ainsi à la société de retracer les parcours de soin des personnes sur les douze derniers mois, ce qui fait courir un risque encore plus important de levée du pseudonymat.

75. Dans la mesure où les trois critères prévus dans l'Avis 05/2014 sur les techniques d'anonymisation, précité, ne sont pas remplis, la formation restreinte en conclut qu'il convient d'évaluer in concreto le risque de réidentification pour établir le caractère anonyme ou pseudonyme des données.

76. En ce sens, elle observe que le rapporteur est parvenu, dans le cadre de ses écritures, à retracer le parcours d'un enfant de douze ans en ALD à partir d'un jeu de données réduit transmis par la société. Elle relève que pour ce faire, il y a consacré peu de temps et peu de moyens : le rapporteur a mené une analyse à partir des données communiquées par la société en utilisant uniquement le logiciel Excel et la nomenclature communiquée par celle-ci afin d'associer les codes alphanumériques à des informations sur le patient et les actes médicaux prodigués. Dans ce cadre, le rapporteur n'a pas eu recours à des sources de données tierces, par exemple à des données des courtiers en données (data brokers) ou encore à des données de géolocalisation. Or, la formation restreinte constate qu'il ressort de la doctrine citée par le rapporteur dans ses écritures qu'il est possible de réidentifier une part significative de personnes dans un jeu de données pseudonymisées à partir de données de géolocalisation (voir notamment les études Unique in the Shopping Mall: On the Re-identifiability of Credit Card Metadata de Yves-Alexandre de MONTJOYE ou encore GeoTrouveTous – projet de réidentification par géolocalisation du laboratoire d'innovation numérique de la CNIL).

77. La formation restreinte relève ainsi qu'une corrélation entre des données tierces et les informations détenues par la société CEGEDIM SANTÉ (notamment les données relatives au patient et les informations relatives à ses consultations) augmenterait considérablement les possibilités de levée du pseudonymat. Si la société conteste détenir des informations géographiques, la formation restreinte rappelle qu'un code région était collecté jusqu'en 2022 et qu'elle détient par ailleurs une table de correspondance entre les numéros de panel des médecins et l'identité de ces derniers.

78. La société conteste également en défense la possibilité de recourir à des données de tiers pour apprécier le caractère anonyme ou non d'un jeu de données. Or, la formation restreinte rappelle à cet égard que la CJUE a jugé qu'afin de qualifier une information de donnée à caractère personnel, il n'est pas nécessaire que cette information permette, à elle seule, d'identifier la personne concernée. Elle a également estimé que le fait que des informations supplémentaires, y compris des contributions extérieures, sont nécessaires pour identifier la personne concernée, n'est pas de nature à exclure que les données en cause puissent être qualifiées de données à caractère personnel (arrêts OC c/ Commission européenne , §§ 47 et 55, et IAB Europe c/ Gegevensbeschermingsautoriteit , § 51, précités).

79. La formation restreinte souligne en tout état de cause que si le rapporteur est parvenu à isoler un individu et à suivre une partie de son parcours de soins avec un tel niveau de détail, à partir d'un extrait seulement d'un jeu de données considérablement plus riche, et de surcroît sans avoir recours à des informations supplémentaires, alors il apparaît possible de lever le pseudonymat des individus par des moyens raisonnables. La formation restreinte relève à ce titre la richesse des données détenues par la société : elle a reçu plus de […] lignes entre le 1er janvier 2021 et le 2 avril 2021 (une ligne correspondant à un événement, par exemple une consultation), détenait […] codes patients sur la période de janvier à mars 2021 et […] codes prescripteurs en avril 2021.

80. Par ailleurs, si le rapporteur n'a pas nommément levé le pseudonymat de l'enfant dont il a suivi une partie du parcours de soins, la formation restreinte rappelle que cette condition n'est pas nécessaire à la qualification de donnée à caractère personnel. En effet, la CJUE a jugé dans l'arrêt OC c/ Commission qu'il n'est pas nécessaire d'apporter la preuve d'une identification effective, puisqu' une telle condition n'est pas prévue à l'article 3, point 1, du règlement 2018/1725, celui-ci se limitant à exiger qu'une personne soit identifiable (§ 61). La formation restreinte considère qu'il convient de raisonner par analogie s'agissant du RGPD, puisque la définition posée à l'alinéa 1 de l'article 4 du RGPD est exactement la même.

81. En troisième lieu, la formation restreinte rappelle que lorsque les trois critères posés par l'avis du G29 précité ne sont pas remplis, la société doit mener une analyse pour être en mesure de démontrer que les risques de réidentification

induits par le processus sont négligeables. Or, la société n'a pas mené une telle analyse s'agissant des constats faits au moment du contrôle de la CNIL. Ce n'est qu'en octobre 2023 que la société indique avoir mené une telle analyse, laquelle ne vaut donc que pour le traitement des données postérieur à 2022. De surcroît, pour évaluer les risques de réidentification, la formation restreinte relève que la société a fait le choix de ne combiner qu'un nombre réduit de données parmi l'ensemble des données dont elle dispose, rendant ainsi le résultat de son étude insuffisamment fiable (en l'espèce, elle a choisi de ne combiner dans son évaluation que l'année de naissance du patient, son sexe et l'information selon laquelle il a ou non des enfants, alors qu'elle disposait de très nombreuses autres données dont notamment le poids et la taille approximatifs, l'historique des consultations, les prescriptions et leur durée, les antécédents médicaux, les constantes physiologiques (glycémie, tension, etc.) et les pathologies diagnostiquées).

82. S'agissant des conclusions de l'évaluation menée par la société […], fournie lors du contradictoire, la formation restreinte considère qu'elles ne remettent pas en cause cette appréciation. En effet, l'évaluation ne porte pas sur le traitement tel que constaté au jour du contrôle mais uniquement sur celui mis en œuvre postérieurement, lequel inclut de nouvelles mesures, consistant notamment en l'appauvrissement de la profondeur des données traitées. Dès lors, l'évaluation ne permet pas de démontrer l'anonymat des données au jour du contrôle.

83. En tout état de cause, la formation restreinte relève que l'expertise de la société […] n'intègre pas, dans son évaluation de la robustesse des techniques de dé-identification […] et des résultats obtenus quant à l'anonymat des ensembles de données , l'ensemble des facteurs permettant de représenter la richesse des données telle qu'elle résulte du suivi durant plusieurs années des mêmes personnes.

84. Enfin et surtout, la formation restreinte note que l'expertise de la société […] arrive à la même conclusion que le rapporteur s'agissant de la possibilité d'isoler un individu dans la base détenue par la société CEGEDIM SANTÉ, l'expertise arrivant également à la conclusion que le k-anonymat est égal à 1, c'est-à-dire qu'il est possible d'isoler un individu dans la base de données. Le k-anonymat est en effet un modèle de mesure de la confidentialité garantissant qu'il existe pour chaque identifiant au sein d'un jeu de données une classe d'équivalence correspondante contenant au moins K-enregistrements. La formation restreinte constate ainsi que bien que l'expertise […] ne conclut pas à la possibilité de réidentification des individus, elle conclut à la possibilité d'isoler un individu dans le jeu de données, ce qui correspond déjà au premier des trois types de risques identifiés par le G29 dans son Avis 05/2014 sur les techniques d'anonymisation du 10 avril 2014 précité.

85. La seconde phase de l'expertise consiste à effectuer une analyse de risques pour étudier quelle est la vraisemblance que les données détenues par la société soient rendues accessibles, par exemple, en cas de violation de données, à des personnes en capacité de rattacher ces données aux identités exactes des patients. La formation restreinte relève le haut niveau de sécurité mis en avant par la société. En revanche, elle conclut que l'exercice mené porte sur le risque d'accès aux données et de probabilité de violation des données. Or, le niveau de sécurité mis en place afin d'assurer la confidentialité des données, aussi élevé soit-il, est sans incidence sur la qualification des données traitées.

86. Il résulte de l'ensemble de ce qui précède qu'au jour du contrôle et jusqu'en 2022, les données directement identifiantes étaient remplacées par des données indirectement identifiantes, à savoir un identifiant unique pour le patient concerné, ce qui permettait de traiter ses données sans pouvoir l'identifier de manière directe. Néanmoins, le pseudonymat pouvait être levé tant la richesse des informations était importante.

87. Dès lors, la formation restreinte considère que les données traitées par la société CEGEDIM SANTÉ jusqu'en 2022 sont pseudonymes et non anonymes.

88. La formation restreinte prend note des mesures complémentaires mises en place par la société depuis 2022, à savoir qu'elle ne collecte plus certaines données et que, pour d'autres, elle ne collecte plus le même niveau de granularité. La société estime qu'ainsi modifié, son traitement est anonyme. Cependant, la formation restreinte estime que l'analyse de l'état nouveau du traitement n'était pas l'objet initial de la procédure et qu'elle n'est pas en état de se prononcer sur ce point dans le cadre de la présente décision. Elle invite la société, si elle le souhaite, à saisir la CNIL d'une demande de conseil pour qu'il soit statué sur le caractère anonyme ou non de la base dans son nouvel état.

2) Sur la qualification du traitement en entrepôt de données de santé

89. La société soutient que le traitement qu'elle met en œuvre n'est pas un entrepôt de données de santé, mais un réseau de médecins qui acceptent de transmettre des données anonymes issues de leurs dossiers médicaux aux partenaires de la société CEGEDIM SANTÉ, à savoir les sociétés […] et […]. Elle estime notamment que la nature transitoire du flux, dans lequel les données ne sont conservées que trois mois, démontre qu'il ne s'agit pas d'une base de données pérenne tel un entrepôt.

90. La formation restreinte rappelle que la notion d'entrepôt de données de santé n'est pas dans la loi Informatique et Libertés mais constitue une construction doctrinale de la CNIL pour l'application des articles 65 et suivants de cette loi. Elle s'apprécie à l'aide d'un faisceau d'indices prenant en compte notamment, mais pas uniquement, la durée de conservation

des données. Parmi les éléments déterminants d'une qualification en entrepôt de données de santé figurent ceux de la réutilisation des données dans des traitements ultérieurs, de l'alimentation au fil de l'eau de la base ainsi que des finalités du traitement.

91. En l'espèce, la formation restreinte constate qu'il ressort des pièces du dossier que la société CEGEDIM SANTÉ :

- collecte massivement des données de santé de patients et de médecins (plus de […] lignes reçues dans la base entre le 1er janvier 2021 et le 2 avril 2021 - une ligne correspondant à un événement, par exemple une consultation ; […] codes patients détenus sur la période de janvier à mars 2021 ; […] codes prescripteurs détenus en avril 2021) ;

- alimente sa base au fil de l'eau, afin d'obtenir un volume important de données (remontée journalière des données depuis les postes des médecins) ;

- met les données à disposition de ses clients qui réalisent des études et des statistiques dans le domaine de la santé. Figure parmi ces clients la société […].

92. La formation restreinte prend acte des modifications substantielles apportées au traitement et effectives au 1er juin 2024. Plus particulièrement, la remontée des données depuis le poste des médecins vers la société […] n'est plus opérée par l'intermédiaire de la société CEGEDIM SANTÉ. Depuis la fin du mois de juillet 2024, la société CEGEDIM SANTÉ n'intervient plus dans la gestion du flux CROSSWAY issu des logiciels des médecins, ces derniers alimentant directement la base […] détenue par la société […].

93. Au regard de ce qui précède, la formation restreinte estime que la société se constituait un entrepôt de données de santé au moment du contrôle par la CNIL et ce, jusqu'à la réorganisation effective au 1er juin 2024 par laquelle les données ne transitent plus via CEGEDIM SANTÉ.

3) Sur le statut de la société en termes de responsabilité de traitement

94. Aux termes de l'article 4 du RGPD, le responsable du traitement est 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 (point 7) et le sous-traitant est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement (point 8).

95. À titre d'éclairage, dans ses lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD, adoptées le 7 juillet 2021, le CEPD explicite la définition du responsable de traitement en ces termes : La détermination des finalités et des moyens revient à décider respectivement du "pourquoi" et du "comment" du traitement : pour une opération de traitement particulière, le responsable du traitement est l'acteur qui a déterminé la raison pour laquelle le traitement a lieu (c'est-à-dire "à quelles fins" ou "pourquoi") et comment cet objectif sera atteint (c'est-à-dire quels moyens doivent être mis en œuvre pour atteindre l'objectif). Une personne physique ou morale qui exerce cette influence sur le traitement de données à caractère personnel participe ainsi à la détermination des finalités et des moyens du traitement en question, conformément à la définition énoncée à l'article 4, paragraphe 7, du RGPD. Le responsable du traitement doit décider à la fois des finalités et des moyens du traitement […]. (§§ 35 et 36).

96. S'agissant de la sous-traitance, les lignes directrices précitées précisent que L'article 4, paragraphe 8, du RGPD définit un sous-traitant comme étant la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement et que Pour être considéré comme un sous-traitant, deux conditions de base doivent être satisfaites :

a) être une entité distincte du responsable du traitement et

b) traiter des données à caractère personnel pour le compte du responsable du traitement (§§ 73 et 76).

97. Le rapporteur considère que la société CEGEDIM SANTÉ définit les finalités et moyens du traitement en cause et constitue un entrepôt de données de santé pour les besoins de sa propre activité, pour mettre ensuite les données à disposition de ses clients qui les réutilisent dans le cadre d'études et de statistiques dans le domaine de la santé.

98. En défense, la société indique intervenir en tant que sous-traitant, d'une part, des médecins utilisant le logiciel CROSSWAY et, d'autre part, des sociétés […] et […] pour lesquelles elle opère le flux CROSSWAY. Elle fait valoir que la détermination des finalités et moyens du traitement invoquée par le rapporteur ne vaut que pour la gestion et le recrutement d'un panel de médecins par la société CEGEDIM SANTÉ, et non pour l'obtention des données des patients de ces derniers. Ainsi, elle soutient ne pas poursuivre de finalités propres pour l'usage des données issues de ce flux et limiter son intervention à un rôle d'intermédiaire technique pour la remontée des données du flux CROSSWAY depuis le poste des médecins vers les sociétés partenaires.

99. La société cite à l'appui de ses déclarations un courrier de clôture de contrôle du 26 novembre 2014 à l'encontre de la société CEGEDIM LOGICIELS MEDICAUX FRANCE (dissoute en 2021 et dont l'intégralité de l'activité a été reprise par la société CEGEDIM SANTÉ) dans lequel la CNIL aurait reconnu à la société ce statut de sous-traitant. Elle estime que ce courrier trouve toujours à s'appliquer dans la mesure où les circonstances de fait et de droit, applicables à la qualification des parties n'ont pas évolué et que le courrier constitue un acte valablement adopté par une personne ayant autorité pour représenter et engager la CNIL, à savoir la Présidente de la Commission. En outre, elle soutient que l'ancienneté du courrier ne saurait être un argument valable dans la mesure où l'acception de la notion d'anonymat n'a pas été modifiée de manière substantielle par le RGPD ou la loi Informatique et Libertés depuis.

100. En premier lieu, la formation restreinte relève que dans l'analyse d'impact qu'elle a conduit, la société s'est désignée en qualité de responsable du traitement de son observatoire et non uniquement pour le recrutement du panel de médecins. Il ressort par ailleurs des pièces du dossier que la société CEGEDIM SANTÉ encadre par des contrats la collecte de données auprès des médecins éligibles souhaitant adhérer à son observatoire épidémiologique , et définit également les modalités de transmission de ces données à ses partenaires […] et […].

101. S'agissant des finalités du traitement, la formation restreinte note que la société détermine le périmètre et les finalités de l'utilisation des données de son observatoire vis-à-vis de ses partenaires. Plus particulièrement, le contrat conclu avec la société […] stipule que l'usage autorisé [des données] est le suivant : réalisation directement ou par personne interposée d'analyses ou études liées à la santé et l'avenant au contrat conclu avec la société […] prévoit notamment qu'elle n'utilisera les données relatives aux prescriptions médicales transmises par CLM [CEGEDIM SANTÉ] que pour réaliser des études. Les résultats des études ne seront commercialisés que sous la forme de statistiques. Toute autre forme de commercialisation des données est interdite (traduction libre). Par ailleurs, la société définit le périmètre des participants à l'observatoire en proposant l'adhésion et l'utilisation du logiciel CROSSWAY à un panel représentatif de médecins de ville, éligibles en fonction de critères géographiques, d'âges et de spécialités.

102. S'agissant des moyens du traitement, la formation restreinte relève que les contrats conclus entre la société et les médecins panélistes ne portent pas uniquement sur le simple recrutement des médecins mais détaillent les moyens du traitement, dont les modalités de collecte et de transmission des données. Tels que conçus, les contrats imposent par exemple aux médecins les conditions de participation au réseau et de transmission des données à la société, notamment s'agissant des catégories de données qui sont collectées, des modalités de communication des données et de la fréquence de leur collecte.

103. La formation restreinte considère qu'il ressort des pièces du dossier que la société CEGEDIM SANTÉ détermine les finalités et les moyens du traitement en cause, qu'elle organise le traitement pour répondre à ses propres besoins et afin de mettre en œuvre son observatoire et qu'elle ne reçoit pas de directive à exécuter.

104. La formation restreinte précise que la transmission des données à des partenaires tiers, qui réutiliseront les données pour leur propre compte, ne fait pas obstacle à la qualification de responsable de traitement de la société CEGEDIM SANTÉ. En cas de traitements en chaîne , chacune des sociétés intervient en tant que responsable de traitement, déterminant les moyens pour le traitement qu'elle met en œuvre pour les finalités qui lui sont propres.

105. En second lieu, la formation restreinte estime que le traitement ne peut être apprécié qu'en tenant compte des constats effectués lors de la mission de contrôle du 30 mars 2021 et à la lumière de la doctrine et de l'état de l'art actuels. La formation restreinte ne s'estime pas liée par les constats effectués lors de la mission de contrôle de 2012.

106. La formation restreinte relève d'abord que le droit à la protection des données à caractère personnel a connu des évolutions conséquentes depuis le courrier de clôture de contrôle adressé à la société CEGEDIM LOGICIELS MEDICAUX FRANCE en 2014, lequel faisait suite à des missions de vérifications menées en 2001 et mars 2012. Ce courrier est par ailleurs antérieur à l'entrée en vigueur du RGPD, texte de référence en matière de protection des données à caractère personnel. Les évolutions de la doctrine s'expriment particulièrement dans la terminologie utilisée, le courrier faisant mention de l'anonymat du patient , à un moment où la notion d'anonymat faisait référence à l'absence de données directement identifiantes, et non à l'impossibilité d'identifier une personne physique à partir d'un jeu de données.

107. La formation restreinte observe ensuite qu'il ne ressort pas de ce courrier que la CNIL estimait, au regard de ses missions de vérification en 2002 puis en 2014, qu'il s'agissait d'un traitement de données anonymisées ne relevant pas du champ d'application de la loi Informatique et Libertés. Si tel avait été le cas, elle n'aurait pas énuméré dans son courrier de clôture un certain nombre de recommandations à mettre en œuvre afin d'assurer la sécurité des données traitées. Or, le courrier invitait notamment la société à mettre en œuvre un mécanisme de purge automatique des fichiers conservés sur les postes des médecins ou encore à désigner un correspondant Informatique et Libertés .

108. En tout état de cause, la formation restreinte rappelle qu'il incombe au responsable de traitement de prendre en compte les évolutions doctrinales et de réévaluer régulièrement les mesures techniques et organisationnelles du traitement mis en œuvre.

109. En conclusion, la formation restreinte ne remet pas en cause la validité du courrier de 2014 mais, tenant compte de son ancienneté et des évolutions du cadre légal et jurisprudentiel, elle estime ne pas être liée par cette position ancienne, position reposant elle-même sur une délibération de la CNIL vieille de plus de vingt ans et des constats afférents. La formation restreinte considère que ce courrier ne saurait démontrer à lui seul la qualité de sous-traitant de la société CEGEDIM SANTÉ.

110. Au vu de l'ensemble de ce qui précède, la formation restreinte considère que la société CEGEDIM SANTÉ est responsable du traitement au sens de l'article 4, point 7, du RGPD. Dès lors, en mettant en œuvre le traitement en cause, la société, si elle collecte et traite des données à caractère personnel en qualité de responsable du traitement, doit se conformer à la règlementation relative à la protection des données à caractère personnel.

C. Sur le manquement à l'article 66 de la loi Informatique et Libertés

111. L'article 65 de la loi Informatique et Libertés prévoit que les traitements contenant des données concernant la santé des personnes sont soumis à la Section 3 : Traitements de données à caractère personnel dans le domaine de la santé du Chapitre III : Obligations incombant au responsable de traitement et au sous-traitant , à l'exception de différentes catégories de traitements, listées aux alinéas 1 à 6 de cet article.

112. L'article 66 de la loi Informatique et Libertés dispose pour sa part :

I - Les traitements relevant de la présente section ne peuvent être mis en œuvre qu'en considération de la finalité d'intérêt public qu'ils présentent. La garantie de normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux constitue une finalité d'intérêt public.

II - Des référentiels et règlements types, au sens des b et c du 2° du I de l'article 8, s'appliquant aux traitements relevant de la présente section sont établis par la Commission nationale de l'informatique et des libertés, en concertation avec la plateforme des données de santé mentionnée à l'article L. 1462-1 du code de la santé publique et des organismes publics et privés représentatifs des acteurs concernés.

Les traitements conformes à ces référentiels peuvent être mis en œuvre à la condition que leurs responsables adressent préalablement à la Commission nationale de l'informatique et des libertés une déclaration attestant de cette conformité. […]

III - Les traitements mentionnés au I qui ne sont pas conformes à un référentiel mentionné au II ne peuvent être mis en œuvre qu'après autorisation de la Commission nationale de l'informatique et des libertés. La demande d'autorisation est présentée dans les formes prévues à l'article 33. […] .

113. Ainsi, en vertu du III de l'article 66 de la loi Informatique et Libertés, les traitements de données à caractère personnel dans le domaine de la santé, dont font partie les entrepôts de données de santé, ne peuvent être mis en œuvre qu'après autorisation de la CNIL ou à la condition d'être conformes à un référentiel mentionné au II de cet article et ce, au regard de l'intérêt public qu'ils présentent.

114. Le rapporteur considère que la société collecte des données pseudonymisées issues des dossiers patients informatisés, transmis par les médecins panélistes via le flux CROSSWAY, afin de se constituer cet entrepôt de données de santé. En l'absence de recueil du consentement des personnes concernées au versement de leurs données dans un entrepôt de données de santé (en application de l'article 9, paragraphe 2, a) du RGPD), la constitution d'un tel entrepôt est soumise à formalités préalables auprès de la CNIL. Or, le rapporteur rappelle que la société CEGEDIM SANTÉ n'a pas recueilli le consentement explicite des personnes concernées par la collecte, l'enregistrement et la conservation des données de santé comprises dans l'entrepôt, n'a présenté aucune demande d'autorisation concernant le traitement en cause et n'a adressé à la CNIL aucune déclaration attestant de la conformité du traitement à un référentiel au sens du paragraphe II de l'article 66 de la loi Informatique et Libertés. Le rapporteur en conclut que la société a méconnu les obligations prévues à l'article 66 de la loi Informatique et Libertés dans le domaine de la santé.

115. En défense, la société soutient qu'un manquement à l'article 66 de la loi Informatique et Libertés n'est pas constitué dans la mesure où elle ne traite pas de données à caractère personnel, y compris des données pseudonymes ou des données de santé. Elle soutient que le flux CROSSWAY ne contient que des données anonymes et que dès lors, elle ne constitue pas un entrepôt de données de santé et n'a pas à procéder aux formalités prévues par l'article 66 de la loi Informatique et Libertés pour pouvoir traiter lesdites données.

116. Par ailleurs, elle considère qu'il ne peut lui être reproché d'avoir méconnu ses obligations dans la mesure où le cadre juridique applicable, surtout la définition de la notion d'anonymisation , manque de clarté. La société soutient notamment qu'il ne peut lui être reproché de ne pas avoir saisi la CNIL d'une demande de conseil car la CNIL n'a jamais fait état de la possibilité pour les organismes de la saisir pour valider les méthodes d'anonymisation employées et qu'en tout état de cause, elle a, de bonne foi, considéré que les données qu'elles traitaient étaient anonymes.

117. À titre liminaire, la formation restreinte note que la CNIL a procédé à certaines publications sur son site web antérieurement au contrôle, par exemple sur la définition d'une donnée de santé (début 2018), les formalités à réaliser pour le traitement de données de santé (début 2018) ou encore la distinction entre un entrepôt de données de santé et une recherche (fin 2019). En plus de ses propres ressources, la CNIL relaye d'autres sources d'informations comme elle l'a par exemple fait avec l'Avis 05/2014 sur les techniques d'anonymisation du G29. Comme elle l'a déjà souligné, la formation restreinte rappelle également que le cadre juridique est avant tout posé par les législateurs français et européen.

118. Dès lors, la formation restreinte considère que la société ne pouvait pas ignorer, au jour du contrôle, le régime juridique applicable à l'entrepôt de données de santé qu'elle se constitue, d'autant plus que d'autres sociétés qui mettent en œuvre des traitements similaires sur le même marché ont demandé des autorisations à la CNIL et que ces autorisations sont publiques et accessibles sur le site web www.legifrance.gouv.fr . Si la société considère que ces autorisations ne sont pas comparables à la base de données qu'elle se constitue, notamment au regard de la richesse des données collectées par ces sociétés, la formation restreinte rappelle que dès lors qu'un organisme se constitue un entrepôt de données de santé, il est tenu de se conformer à ses obligations et notamment à l'article 66 de la loi Informatique et Libertés, peu importe la richesse de l'entrepôt et la granularité des données collectées.

119. La formation restreinte rappelle que, pour les raisons exposées ci-avant, la société CEGEDIM SANTÉ traitait, au jour du contrôle, des données de santé de manière pseudonymisée pour se constituer un entrepôt de données de santé, de sorte qu'elle était tenue de respecter le RGPD et la loi Informatique et Libertés.

120. En premier lieu, la formation restreinte relève que la seule exception prévue aux obligations de l'article 65 de ladite loi susceptible de s'appliquer en l'espèce est celle relative au cas dans lequel la personne concernée a donné son consentement explicite au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques, conformément à l'article 65 1°, renvoyant à l'alinéa a) de l'article 9, paragraphe 2, du RGPD. Or, en l'espèce, dans la mesure où la société CEGEDIM SANTÉ considère ne pas traiter de données à caractère personnel, elle n'a mis en œuvre aucune mesure pour se conformer aux règles applicables en matière de traitement de ces données. En particulier, la société n'a mis en œuvre aucun mécanisme de recueil du consentement explicite et préalable des patients des médecins du panel pour le traitement en cause.

121. En conséquence, la formation restreinte considère que, dès lors que la société traitait des données de santé au jour du contrôle et qu'elle ne peut se prévaloir d'aucune des exceptions prévues à l'article 65 de la loi Informatique et Libertés, le traitement qu'elle met en œuvre est soumis à la section 3 du chapitre III de la loi Informatique et Libertés.

122. En deuxième lieu, la formation restreinte relève qu'en l'espèce, la société ne s'est pas conformée aux exigences de l'article 66 de la loi Informatique et Libertés pour se constituer un entrepôt de données de santé.

123. Tout d'abord, elle relève que la société n'a formulé aucune demande d'autorisation visant à ce que le traitement en cause soit considéré comme nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique ou nécessaire à des fins de recherche scientifique.

124. Ensuite, la formation restreinte rappelle qu'en l'absence d'autorisation de la CNIL, un traitement de données à caractère personnel dans le domaine de la santé peut également être mis en œuvre s'il est conforme à un référentiel au sens du II de l'article 66 de la loi Informatique et Libertés, à condition que le responsable du traitement adresse préalablement à la CNIL une déclaration attestant de cette conformité. La formation restreinte constate que ce n'est pas le cas en l'espèce et que la société n'a adressé à la CNIL aucune déclaration attestant de cette conformité.

125. En troisième lieu, la formation restreinte prend acte des nouvelles mesures mises en œuvre postérieurement au contrôle.

126. D'une part, la société a indiqué qu'elle ne collectait plus certaines données depuis 2022. Cependant, comme développé ci-avant, la formation restreinte considère que les éléments communiqués par la société en cours de procédure ne lui permettent pas de s'assurer qu'elle traite désormais des données anonymes. Elle relève par ailleurs, en tout état de cause, que les mesures déployées en 2022 ne sauraient exonérer la société de sa responsabilité pour le passé.

127. D'autre part, la société a indiqué qu'à compter de la fin du mois de juillet 2024, elle n'interviendrait plus dans la gestion du flux CROSSWAY, qui alimente désormais directement la base […] détenue par la société […]. Ainsi, les données du flux CROSSWAY ne transitent plus via la société CEGEDIM SANTÉ.

128. Au vu de l'ensemble de ce qui précède, la formation restreinte considère que la société traitait des données de santé au jour du contrôle et jusqu'à juillet 2024 et qu'elle aurait dû se conformer aux exigences de l'article 66 de la loi du 6 janvier 1978 modifiée pour se constituer un entrepôt de données de santé.

129. Par conséquent, la formation restreinte considère que la société a manqué à ses obligations en traitant des données à caractère personnel dans le domaine de la santé en violation de l'article 66 de la loi du 6 janvier 1978 modifiée.

130. Au regard des mesures prises par la société au cours de la procédure, la formation restreinte considère qu'il n'y a pas lieu de prononcer une injonction de mise en conformité avec les dispositions de l'article 66 précité, comme le proposait le rapporteur, la société n'intervenant plus à ce jour dans la gestion du flux CROSSWAY.

D. Sur le manquement à l'article 5, paragraphe 1, a) du RGPD

131. Aux termes de l'article 5, paragraphe 1, a) du RGPD, Les données à caractère personnel doivent être :

a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence) .

132. L'article L. 162-4-3 du code de la sécurité sociale dispose que les médecins peuvent, à l'occasion des soins qu'ils délivrent et sous les conditions prévues à l'article L. 161-31, consulter les données issues des procédures de remboursement ou de prise en charge qui sont détenues par l'organisme dont relève chaque bénéficiaire de l'assurance maladie. Dans ce cas, ils en informent préalablement le patient. Le bénéficiaire des soins donne son accord à cet accès en permettant au médecin d'utiliser, à cet effet, le moyen d'identification électronique mentionné à l'article L. 161-31. Le relevé des données mis à la disposition du médecin contient les informations nécessaires à l'identification des actes, produits ou prestations pris en charge pour les soins délivrés en ville ou en établissement de santé, au regard notamment des listes mentionnées aux articles L. 162-1-7, L. 165-1 et L. 162-17. Il comporte également le code prévu pour les identifier dans ces listes, le niveau de prise en charge et, pour les patients atteints d'une affection de longue durée, les éléments constitutifs du protocole de soins mentionné au septième alinéa de l'article L. 324-1. […] .

133. L'article R. 162-1-10 du même code dispose quant à lui que Pour l'application de l'article L. 162-4-3, les organismes gestionnaires des régimes de base d'assurance maladie assurent, à l'usage des médecins conventionnés ou exerçant leur activité dans un établissement ou un centre de santé, à l'occasion des soins qu'ils délivrent, la mise en œuvre d'un service de consultation par voie électronique des informations afférentes aux prestations délivrées à leurs bénéficiaires .

134. Pour la mise en œuvre de ces dispositions, l'assurance maladie a mis en place, notamment, deux téléservices :

- le téléservice HRi : informations relatives à l'historique des remboursements de santé effectués par l'assurance maladie pour un patient sur les douze derniers mois ;

- le téléservice ALDi : données relatives aux affections longue durée (ALD) reconnues par l'assurance maladie pour un patient (notamment la date de la consultation, le code de l'ALD, les dates de début et de fin de l'ALD et l'information selon laquelle l'ALD est prise en charge).

135. En l'espèce, la délégation de contrôle a constaté que, parmi les données transmises par le flux CROSSWAY à la société CEGEDIM SANTÉ, figurent des données issues de ces deux téléservices.

136. La délégation a par ailleurs été informée que les informations transmises à la société CEGEDIM SANTÉ par l'intermédiaire du flux CROSSWAY peuvent être issues de l'interrogation des téléservices ou avoir été directement renseignées par les médecins.

137. Le rapporteur soutient que les dispositions du code de la sécurité sociale et du code de la santé publique prévoient uniquement un droit de consultation des données contenues dans les téléservices mis en place par la Caisse nationale d'assurance maladie (CNAM) par des professionnels habilités. Elles ne prévoient pas la possibilité pour un acteur privé, par l'intermédiaire du médecin, de collecter directement ces données depuis les téléservices. Ainsi, le rapporteur estime que la collecte de ces données par CEGEDIM SANTÉ est illicite et effectuée en violation de l'article 5, paragraphe 1, a) du RGPD.

1) Sur les données issues du téléservice ALDi

138. La formation restreinte rappelle que les dispositions du code de la sécurité sociale régissent uniquement les modalités d'accès direct aux données personnelles issues du téléservice ALDi, mais ne prescrivent pas l'accès à ces mêmes données depuis les dossiers informatisés des médecins. La CNIL a d'ailleurs autorisé par le passé des extractions pseudonymisées des dossiers patients, pour la constitution de bases de données de santé, sans exclure par principe que soient importées dans ces bases des données issues originellement des bases de l'assurance maladie, à condition que le traitement soit proportionné et suffisamment sécurisé, et que les autres règles de traitement des données à caractère personnel soient respectées. Dans ces conditions, la formation restreinte estime que, ainsi que la société le soutient, celle-ci est autorisée à recevoir dans le flux CROSSWAY les données issues du téléservice ALDi dans la mesure où elles sont intégrées au dossier informatisé du patient du médecin par le médecin lui-même, au même titre que les autres données qui y sont enregistrées.

139. Or, il ressort des pièces du dossier que l'extracteur CROSSWAY a pour seul objet de permettre l'extraction des données issues des dossiers informatisés des patients mais ne procède à aucune connexion au téléservice et n'en aspire pas les données directement. En particulier, la société fait valoir que le médecin peut, dans un premier temps, consulter les

données issues du téléservice ALDi sans les télécharger et, dans un second temps, décider de télécharger ces données et de les verser au dossier patient informatisé du logiciel CROSSWAY.

140. La formation restreinte prend acte des éléments apportés par la société et estime que le manquement à l'article 5, paragraphe 1, a) du RGPD n'est pas constitué s'agissant de la collecte de données issues du téléservice ALDi.

2) Sur les données issues du téléservice HRi

141. S'agissant des données issues du téléservice HRi, la société soutient en défense que les dispositions du code de la sécurité sociale ne prévoient pas de règles qui prescrivent ou interdisent l'accès aux dossiers informatisés des médecins contenant des données provenant du téléservice HRi, de surcroît lorsqu'un tel accès ne concerne que des données anonymes. Ainsi, la société estime être autorisée à recevoir ces données dans le flux CROSSWAY, au même titre que les autres données qui figurent dans les dossiers patients.

142. Plus particulièrement, la société fait valoir que les données issues du téléservice HRi sont enregistrées dans le flux CROSSWAY en local sur le poste du médecin, par le médecin lui-même au moment de la consultation du téléservice, et que ce n'est que dans un second temps que les données sont récupérées par l'extracteur CROSSWAY. Elle en conclut que l'extracteur CROSSWAY ne procède à aucune aspiration directe de ces données et que la collecte ne peut donc être considérée comme illicite. Cependant, la société a indiqué être disposée, à titre subsidiaire et dans l'hypothèse où la formation restreinte retiendrait la position du rapporteur, à faire évoluer le logiciel CROSSWAY dans un sens où le téléchargement des données HRi n'interviendrait que sur option activable par les médecins.

143. En tout état de cause, la société insiste sur sa transparence et sa bonne foi, soutenant que la CNIL avait connaissance des modalités de remontée des données d'historique de remboursement auprès de la société CEGEDIM LOGICIELS MEDIDAUX, puis CEGEDIM SANTÉ. Elle produit à l'appui de sa défense un courrier daté du 25 avril 2013 dans lequel la société CEGEDIM LOGICIELS MEDIDAUX informait la CNIL de l'intégration dans le logiciel des médecins d'une fonctionnalité permettant la conservation des données issues de l'historique de remboursement.

144. Enfin, la société insiste sur le fait que l'accès aux données du téléservice HRi par les professionnels de santé est recommandé par le GIE SESAME-Vitale et que, plus globalement, cette fonctionnalité d'accès aux données par les médecins poursuit un objectif de santé publique et de prévention de l'iatrogénie médicamenteuse, afin qu'ils puissent disposer des informations relatives aux médicaments, soins et examens prescrits à leur patient par d'autres médecins.

145. Le rapporteur insiste sur le fait que la difficulté ne réside pas dans le fait que le médecin accède aux données des téléservices HRi et puisse les verser dans le dossier informatisé patient, mais dans le fait qu'à partir du moment où le médecin y accède, la société CEGEDIM SANTÉ se voit transmettre les données automatiquement, sans que le médecin ait jugé nécessaire que ces informations figurent dans le dossier du patient au sein de son logiciel de travail, en procédant lui-même à leur intégration dans le dossier.

146. La formation restreinte constate qu'à la différence des données issues du téléservice ALDi, la consultation des données issues du téléservice HRi par le médecin emporte leur téléchargement automatique, sur une profondeur de douze mois, dans le dossier informatisé du patient du logiciel CROSSWAY.

147. En ne prévoyant pas d'étape intermédiaire par laquelle le médecin peut consulter les données sans que la consultation n'emporte automatiquement le téléchargement dans le dossier patient, la formation restreinte estime que la société CEGEDIM SANTÉ procède à une aspiration automatique des données issues du téléservice HRi dans le flux CROSSWAY, dès que le médecin se connecte au logiciel pour consulter les données et sans aucune action complémentaire de sa part.

148. La formation restreinte estime par ailleurs que le critère de praticité invoqué en défense par la société, selon lequel les médecins ont accès directement aux informations relatives aux médicaments, soins et examens prescrits à leurs patients par d'autres médecins afin de détecter d'éventuelles incompatibilités, ne saurait justifier une utilisation des données de patients allant à l'encontre de la réglementation.

149. La formation restreinte rappelle en outre que ce n'est pas l'accès aux données du téléservice HRi par les médecins ni leur versement au dossier informatisé patient qui est remis en cause, mais le fait que l'extracteur ne prévoit pas de la possibilité de consulter les données sans téléchargement automatique dans le dossier patient et donc, de facto, sans aspiration de ces données par la société CEGEDIM via l'extracteur CROSSWAY. La formation restreinte estime que cette collecte de données intervient en méconnaissance des articles L. 162-4-3 et R. 162-1-10 du code de la sécurité sociale et de l'article R. 1111-8-6 du code de la santé publique, qui ne prévoient pas pour un acteur privé cette possibilité de collecter directement, par l'intermédiaire de la seule consultation par un médecin du téléservice HRi, des données qu'il contient.

150. Enfin, s'agissant du courrier du 25 avril 2013 produit par la société, la formation restreinte relève que celui-ci ne détaille pas les modalités de consultation, de téléchargement dans le dossier patient puis de transmission des données de

l'historique de remboursement à la société CEGEDIM LOGICIELS MEDICAUX. Or, la formation restreinte rappelle que ce n'est pas l'accès aux données par les médecins qui est remis en cause, mais les modalités de leur transmission à la société. Dès lors, le contenu de ce courrier n'est pas de nature à influer sur la caractérisation du manquement.

151. Au regard de ce qui précède, la formation restreinte estime que le manquement à l'article 5, paragraphe 1, a) du RGPD est constitué s'agissant de la collecte de données issues du téléservice HRi.

III. Sur le prononcé de mesures correctrices et la publicité

152. L'article 20, paragraphe IV, de la loi Informatique et Libertés dispose : Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut également, le cas échéant après lui avoir adressé l'avertissement prévu au I du présent article ou après avoir prononcé à son encontre une ou plusieurs des mesures correctrices prévues au III, saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes : […]

2° Une injonction de mettre en conformité le traitement avec les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi ou de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits, qui peut être assortie, sauf dans des cas où le traitement est mis en œuvre par l'État, d'une astreinte dont le montant ne peut excéder 100 000 € par jour de retard à compter de la date fixée par la formation restreinte ; […]

7° A 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 .

153. L'article 83 du RGPD, tel que visé par l'article 20, paragraphe IV, de la loi Informatique et Libertés, prévoit quant à lui 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.

A. Sur le prononcé d'une amende administrative et son montant

154. La société fait valoir qu'elle a de bonne foi considéré qu'elle ne traitait pas de données à caractère personnel. Elle relève qu'une action répressive a été déclenchée à son encontre plus de deux ans après les contrôles sans que la CNIL ne lui ait préalablement notifié sa position divergente sur l'appréciation de la nature des données traitées et ne lui a donc pas donné l'occasion de procéder aux formalités requises. Elle soutient également que la CNIL avait connaissance du traitement mis en œuvre par la société depuis les contrôles menés auprès de CEGEDIM LOGICIELS MEDICAUX en 2002 et 2012 sans qu'il n'ait été demandé à la société de déposer une demande d'autorisation. Enfin, la société indique que, compte tenu de son statut de sous-traitant, elle ne peut être considérée comme responsable des manquements allégués, les dispositions de l'article 66 de la loi Informatique et Libertés et de l'article 5, paragraphe 1, a) du RGPD énonçant des obligations applicables aux responsables de traitement uniquement.

155. S'agissant du montant de l'amende proposé par le rapporteur, la société considère qu'il est disproportionné et qu'il n'est pas démontré comment la part du chiffre d'affaires de la société CEGEDIM SANTÉ relative à l'activité de l'observatoire a été prise en compte dans la détermination de ce montant.

156. En premier lieu, la formation restreinte relève que les manquements constatés aux dispositions de l'article 66 de la loi Informatique et Libertés et de l'article 5, paragraphe 1, a) du RGPD lui sont imputables en sa qualité de responsable du traitement en cause.

157. En deuxième lieu, pour évaluer le bien-fondé du prononcé d'une amende, la formation restreinte souligne qu'il convient 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 du traitement et du nombre de personnes concernées par ce dernier.

158. La formation restreinte considère que les manquements constatés sont graves. En effet, tant le RGPD que la loi Informatique et Libertés prévoient un principe d'interdiction de traitement des catégories particulières de données, dont font partie les données de santé. Le régime prévu par la section 3 (Traitements de données à caractère personnel dans le domaine de la santé) du chapitre III (Obligations incombant au responsable de traitement et au sous-traitant) de la loi Informatique et Libertés constitue donc une exception à ce principe d'interdiction de traitement, qui doit être interprétée strictement. Le strict respect des dispositions de cette section par les responsables de traitements qui souhaitent traiter

des données de santé est donc essentiel pour ne pas porter atteinte aux droits fondamentaux des personnes concernées. Or, en l'espèce, la formation restreinte relève que la société n'a pas respecté les obligations lui incombant en vertu de l'article 66 de la loi du 6 janvier 1978 modifiée. En outre, en collectant les données issues du téléservice HRi, dont l'usage et l'accès sont pourtant strictement encadrés, la société a enfreint le principe de licéité de traitement des données à caractère personnel et ce à des fins commerciales, élément qui doit être pris en compte dans la détermination du montant de l'amende.

159. La formation restreinte relève par ailleurs le caractère massif du traitement. En effet, le nombre de lignes reçues entre le 1er janvier 2021 et le 2 avril 2021 par la société CEGEDIM SANTÉ est de plus de […], ce qui est considérable et démontre l'ampleur du traitement en cause. Cette ampleur et la richesse des données traitées se reflètent également dans leur profondeur historique, la société récupérant via le téléservice HRi des données sur une profondeur de douze mois.

160. En troisième lieu, la formation restreinte estime qu'il ne peut être reproché à la CNIL de ne pas avoir demandé à la société de régulariser son traitement plus tôt, alors qu'elle avait connaissance de celui-ci avant le contrôle réalisé en 2021. La formation restreinte rappelle qu'en application du principe de responsabilité introduit aux articles 5, paragraphe 2, et 24 du RGPD, il appartient aux acteurs de se renseigner sur leurs obligations et de réaliser les démarches nécessaires afin d'être en conformité. La formation restreinte estime en application du critère prévu à l'alinéa b) de l'article 83, paragraphe 2, du RGPD que la société a fait preuve de négligence en considérant qu'elle pouvait, pour mettre en œuvre des traitements de données de santé, s'abstenir de respecter l'article 66 de la loi Informatique et Libertés. Dans la mesure où le traitement de données de santé est l'objet principal et historique de l'activité de la société, la formation restreinte considère que la société ne pouvait pas, de bonne foi, ignorer ses obligations découlant de la règlementation relative à la protection des données à caractère personnel, particulièrement en tant qu'acteur spécialisé dans le domaine de la santé et au regard de la doctrine disponible susmentionnée, d'autant plus que d'autres sociétés mettant en œuvre des traitements similaires sur le même marché ont demandé des autorisations à la CNIL et que ces autorisations sont publiques.

161. En quatrième 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 les manquements.

162. La formation restreinte rappelle que les données concernées sont notamment des données de santé, lesquelles sont des catégories particulières de données au sens de l'article 9 du RGPD, dites données sensibles . Compte tenu de la nature des données en cause, et du secteur dans lequel elle intervient, la formation restreinte considère que la société aurait dû faire preuve d'une vigilance particulière en ce qui concerne le traitement qu'elle met œuvre.

163. En dernier lieu, la formation restreinte relève qu'en application des dispositions de l'article 20, paragraphe IV, de la loi Informatique et Libertés, la société CEGEDIM SANTÉ encourt une sanction financière d'un montant maximum de 20 millions d'euros ou 4 % de son chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Elle relève que le chiffre d'affaires de la société CEGEDIM LOGICIELS MEDICAUX France, dont la société CEGEDIM SANTÉ a repris l'intégralité des activités, était de […] en 2021.

164. Dès lors, au regard des manquements constatés, des capacités financières de la société et des critères pertinents de l'article 83, paragraphe 2, du RGPD évoqués ci-avant, la formation restreinte estime qu'une amende de huit cent mille euros (800 000 €) apparaît justifiée.

B. Sur le prononcé d'une injonction

165. D'une part, s'agissant de l'injonction proposée par le rapporteur d'anonymiser les données ou de mettre en conformité le traitement avec les dispositions de l'article 66 de la loi du 6 janvier 1978 modifiée, la formation restreinte relève que la société a fait part de modifications substantielles du traitement au cours de la procédure de sanction. D'après les informations communiquées par la société dans ses observations en défense, les données du flux CROSSWAY sont désormais transmises directement à la société […], sans l'intermédiaire de la société CEGEDIM SANTÉ.

166. En conséquence, il n'y a, en tout état de cause, pas lieu de prononcer une injonction de mise en conformité avec les dispositions de l'article 66 de la loi du 6 janvier 1978 modifiée pour le traitement opéré par la société CEGEDIM SANTÉ, cette société n'intervenant plus dans ce cadre.

167. D'autre part, la société demande, si la formation venait à retenir le manquement à l'article 5, paragraphe 1, a) du RGPD, que la proposition du rapporteur lui enjoignant de cesser la collecte des données issues du téléservice HRi ne soit pas suivie. Elle propose, à titre subsidiaire, de modifier le logiciel CROSSWAY de manière à supprimer la fonctionnalité de téléchargement automatique des données HRi par les médecins et de ne prévoir un téléchargement de ces données dans le dossier patient que sur action positive des médecins.

168. La formation restreinte prend acte que la société est disposée, en sa qualité d'éditrice du logiciel, à faire évoluer le flux CROSSWAY afin que le traitement soit conforme aux dispositions applicables. En outre, pour les raisons rappelées ci-

dessus, essentiellement liées au fait que la société CEGEDIM SANTE n'est plus depuis ce mois de juillet responsable du traitement mais uniquement éditrice du logiciel, la formation restreinte considère qu'il n'y a pas lieu de prononcer une injonction.

C. Sur la publicité

169. Le rapporteur considère que la publicité de la sanction est nécessaire au regard de la gravité des manquements en cause et du nombre de personnes concernées. Il estime que la publicité contribuera à informer les personnes concernées de l'existence du traitement de leurs données, y compris de données de santé, dont la grande majorité n'a pas connaissance.

170. En défense, la société conteste la proposition du rapporteur de rendre publique la présente décision et fait valoir que si le manquement était aussi grave que le prétend le rapporteur, la CNIL ne l'aurait pas laissé perdurer sans action correctrice depuis 2014. Elle ajoute que la publicité de la délibération lui causerait un préjudice commercial et créerait un risque de divulgation d'informations sur l'hébergement et la transmission des données pouvant porter atteinte à la sécurité des données.

171. La société ajoute qu'elle ne dispose pas des moyens financiers de communiquer auprès des médecins afin de les convaincre de poursuivre leur adhésion à l'observatoire et que, de manière générale, la publicité de la sanction lui ferait encourir un risque réel quant à sa survie et au regard de sa santé financière précaire.

172. Enfin, elle estime que le rapporteur ne saurait utilement invoquer, pour justifier de la publicité de la sanction, la nécessité d'assurer l'information des personnes sur les traitements mis en œuvre par la société, alors qu'il ne retient aucun manquement relatif à l'information des personnes, que les personnes ont été informées individuellement par leur médecin de l'existence du traitement et que la société n'a aucun contact direct avec les personnes concernées.

173. La formation restreinte considère que la publicité de la présente décision se justifie au regard de la gravité des manquements en cause et du nombre de personnes concernées. Elle rappelle qu'en cas de publicité, les informations relevant du secret des affaires, visées à l'article L. 151 du code de commerce, sont occultées des décisions publiées par la formation restreinte. S'agissant de l'argument concernant l'impact d'une publicité sur ces relations avec les médecins partenaires, elle souligne que la société aura la possibilité de communiquer auprès de ses partenaires sur les actions qu'elle aura mises en œuvre pour se conformer à ses obligations.

174. S'agissant de l'information des personnes, la formation restreinte estime que bien qu'il ne soit pas fait grief à la société de ne pas avoir informé les personnes concernées du traitement existant dans la présente procédure, il apparaît essentiel que les personnes concernées aient connaissance des manquements commis par la société afin, notamment, de pouvoir faire valoir leurs droits.

175. La mesure est proportionnée dès lors que la décision n'identifiera plus nommément la société à l'expiration 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 une amende administrative à l'encontre de la société CEGEDIM SANTÉ d'un montant de huit cent mille euros (800 000 €) au regard des manquements à l'article 66 de la loi n° 78-17 du 6 janvier 1978 modifiée et à l'article 5, paragraphe 1, a) du RGPD ;

• 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

M. Philippe-Pierre CABOURDIN

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.