RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Légifrance
Le service public de la diffusion du droit

Délibération SAN-2026-001 du 8 janvier 2026

Commission Nationale de l'Informatique et des Libertés

Nature de la délibération : Sanction
Etat juridique : En vigueur

Date de publication sur Légifrance : Mercredi 14 janvier 2026

Délibération de la formation restreinte n° SAN-2026-001 du 8 janvier 2026 prononçant une sanction pécuniaire à l'encontre de la société FREE MOBILE

Les développements de la délibération comportant des données à caractère personnel ou des secrets protégés par la loi sont remplacés par le signe […]

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de M. Philippe-Pierre CABOURDIN, président, M. Vincent LESCLOUS, vice-président, Mmes Laurence FRANCESCHINI et Isabelle LATOURNARIE-WILLEMS, MM. KLING, membres,

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

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

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

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

Vu la décision n° 2025-1154 QPC du 8 août 2025 du Conseil constitutionnel ;

Vu la décision n° 2024-205C du 6 novembre 2024 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 ;

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 du 17 février 2025 ;

Vu le rapport de M. Tarissan, commissaire rapporteur, notifié à la société le 25 juillet 2025 ;

Vu les observations écrites de la société FREE MOBILE reçues le 15 septembre 2025 ;

Vu la réponse du rapporteur notifiée à la société FREE MOBILE le 15 octobre 2025 ;

Vu les observations écrites de la société FREE MOBILE reçues le 17 novembre 2025 ;

Vu la clôture de l'instruction notifiée à la société FREE MOBILE le 18 novembre 2025 ;

Vu la demande de huis-clos formulée le 15 septembre 2025 et refusée le 3 décembre 2025 ;

Vu les observations orales formulées lors de la séance de la formation restreinte du 15 décembre 2025 ;

Vu la note en délibéré produite par la société le 19 décembre 2025 ;

Vu les autres pièces du dossier,

Étaient présents, lors de la séance de la formation restreinte du 15 décembre 2025 :

- Monsieur Tarissan, commissaire, entendu en son rapport ;

En qualité de représentants de la société FREE MOBILE :

- […]

Le président ayant vérifié l'identité des représentants du mis en cause, présenté le déroulé de la séance et rappelé que le mis en cause peut, s'il le souhaite, présenter des observations orales introductives ou en réponse aux questions des membres de la formation restreinte.

La société FREE MOBILE ayant été informée de son droit de garder le silence sur les faits qui lui étaient reprochés et ayant eu la parole en dernier.

Après en avoir délibéré, a adopté la décision suivante :

I. Faits et procédure

1. Le groupe ILIAD, spécialisé dans les télécommunications en Europe, compte plus de 50,2 millions d'abonnés. La société française ILIAD est la maison mère du groupe du même nom. Elle détient à 100 % la société FREE MOBILE (ci-après la société), qui exerce une activité d'opérateur de téléphonie mobile et comptait, au 31 décembre 2024, environ 15,5 millions d'abonnés mobiles. En 2024, le chiffre d'affaires de la société ILIAD était de 10,024 milliards d'euros pour un résultat net de 367 millions d'euros.

2. La société FREE MOBILE a été alertée le 21 octobre 2024, par un attaquant s'étant introduit dans son système d'information, de la compromission de la confidentialité des données de ses abonnés (y compris d'abonnés convergents c'est-à-dire à la fois clients de la société FREE MOBILE et de la société FREE). A la suite de cette alerte, la société a conduit des investigations qui ont permis de confirmer la survenance d'une violation de données (ci-après la violation de données en cause). Celle-ci a duré du 28 septembre au 22 octobre 2024.

3. La société a notifié cette violation de données à la Commission nationale de l'informatique et des libertés (ci-après la Commission ou la CNIL), le 23 octobre 2024, puis a complété cette notification le 5 novembre 2024. Par ailleurs, elle a informé les personnes concernées de la survenance de la violation de données, par courriel, de manière échelonnée entre le 24 et le 29 octobre 2024 afin de ne pas saturer les serveurs de messagerie.

4. Au jour de la notification du rapport de sanction, la CNIL avait reçu 2 614 plaintes de personnes concernées par cette violation de données.

5. Par décision n° 2024-205C du 6 novembre 2024, la Présidente de la Commission a chargé le secrétaire général de procéder ou de faire procéder à une mission de contrôle afin de vérifier la conformité à la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (ci-après la loi Informatique et Libertés ou LIL) et au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après le RGPD ou le Règlement), de tout traitement mis en œuvre par les sociétés FREE MOBILE et FREE.

6. En application de cette décision, le 8 novembre 2024, une délégation a procédé à une mission de contrôle sur place dans les locaux des sociétés FREE MOBILE et FREE sis 16 rue de la Ville L'Évêque à Paris (75008).

7. Aux fins d'instruction de ces éléments, la présidente de la Commission a, le 17 février 2025, désigné Monsieur Fabien TARISSAN 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.

8. Le 24 juillet 2025, la présidente de la Commission a informé les sociétés FREE MOBILE et FREE de sa décision de disjoindre la procédure de sanction initialement intentée à l'égard des deux sociétés, chacune de celles-ci étant désormais poursuivies dans le cadre d'une procédure distincte.

9. A l'issue de son instruction, le rapporteur a fait notifier le 25 juillet 2025 à la société FREE MOBILE un rapport détaillant les manquements aux articles 5-1-e), 32 et 34 du RGPD 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 mettre en conformité le traitement avec les dispositions des articles 5- 1- e) et 32 du RGPD. Il proposait également que cette décision soit rendue publique.

10. Le 15 septembre 2025, la société a produit des observations en réponse au rapport de sanction.

11. Le rapporteur a répondu aux observations de la société le 15 octobre 2025.

12. Le 17 novembre 2025, la société a produit ses secondes observations en réponse.

13. Par courrier du 18 novembre 2025, le rapporteur a, en application du III de l'article 40 du décret n° 2019-536 susvisé, informé la société et le président de la formation restreinte que l'instruction était close.

14. Par courrier du 18 novembre 2025, la société a été informée que le dossier était inscrit à l'ordre du jour de la séance de la formation restreinte du 4 décembre 2025.

15. Le 18 novembre 2025, la société a, par l'intermédiaire de son conseil, sollicité le report de la séance de la formation restreinte. Le 25 novembre 2025, le président de la formation restreinte a fait droit à cette demande de report et a informé la société de l'inscription du dossier à l'ordre du jour de la séance du 15 décembre 2025.

16. Le 3 décembre 2025, le président de la formation restreinte a refusé la demande de huis-clos formée par la société dans ses observations du 15 septembre 2025. Il a rappelé que la procédure devant la formation restreinte étant écrite et que si la société ne souhaitait pas dévoiler devant des tiers des éléments susceptibles de lui porter préjudice, elle pouvait, lors de la séance, renvoyer à ses observations écrites.

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

II. La violation de données en cause

18. Il résulte de l'enquête menée par la société FREE MOBILE, à la suite de l'alerte reçue le 21 octobre 2024, que l'attaquant s'est d'abord connecté à son réseau privé virtuel (ci-après VPN) […]

19. L'attaquant s'est ensuite connecté à l'outil de gestion des abonnés de la société, […]. Cet outil permet de consulter les données relatives à la relation commerciale des clients de la société FREE MOBILE. Il ne donne pas directement accès aux données brutes mais propose une fonctionnalité recherche à travers un formulaire à remplir (par exemple, saisie d'un nom ou d'un numéro d'abonné). Une fois la recherche lancée, le système interroge la base de données des abonnés mobiles de la société FREE MOBILE, mais également celle des abonnés fixes de la société FREE lorsque les clients sont dits convergents (dans les cas où un client est un abonné à la fois de la société FREE MOBILE et de la société FREE). Le système renvoie uniquement les résultats correspondant à la recherche en les affichant grâce à la fonction consultation . C'est donc cette dernière qui permet d'afficher à l'écran de l'utilisateur les données à caractère personnel spécifiques d'un client à la suite d'une recherche .

20. Une fois connecté à l'outil MOBO, l'attaquant a ainsi pu accéder aux données à caractère personnel d'abonnés de la société, à savoir leurs données d'identité, leurs données de contact, leurs données contractuelles et, pour les clients dits convergents , leur IBAN.

21. Au total, l'attaquant a pu prendre connaissance, des données concernant 24 633 469 contrats, dont 19 460 891 contrats mobiles (FREE MOBILE) et 5 172 577 contrats fixes (FREE).

III. Motifs de la décision

A. Sur la responsabilité de traitement de la société FREE MOBILE

22. Aux termes de l'article 4, alinéa 7, du RGPD, le responsable de 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 .

23. Dans son rapport, le rapporteur souligne que la délégation a été informée lors du contrôle que, dans le cadre de son activité d'opérateur de téléphonie mobile, la société FREE MOBILE dispose de sa propre base de données d'abonnés mobiles, qu'elle alimente avec les données de ses propres clients. Son outil de gestion de clientèle MOBO lui permet d'accéder à sa base de données, ainsi qu'à la base de données d'abonnés fixes gérée par la société FREE pour les clients dits convergents . Lors du contrôle, les sociétés FREE MOBILE et FREE ont indiqué à la délégation être chacune responsable des traitements liés à la gestion de leur clientèle respective, ce qui correspond à ce qui est inscrit dans leurs registres. Le rapporteur n'a pas remis en cause cette qualification juridique dans le cadre de la présente procédure.

24. La société ne conteste pas être responsable du traitement relatif à la gestion de sa propre clientèle. Elle reproche cependant au rapporteur d'imputer indistinctement des manquements aux sociétés FREE MOBILE et FREE, sur la base des mêmes constats, sans prendre en compte leurs traitements et responsabilités respectifs.

25. La formation restreinte relève, à titre liminaire, que la violation de données a touché à la fois le système d'information de la société FREE MOBILE et celui de la société FREE, filiales du même groupe. Lors du contrôle de la CNIL au sein des deux sociétés, celles-ci étaient en partie représentées par les mêmes personnes (notamment, le président et le responsable réseau). Il a été constaté que certaines mesures de sécurité étaient communes aux deux sociétés […].

26. A l'issue de son instruction, le rapporteur a considéré, à l'instar des deux sociétés, que chacune d'elles met en œuvre un traitement relatif à la gestion de ses propres abonnés, à l'aide d'outils qui lui sont propres, dont chacune est responsable de traitement. Au regard des éléments du dossier, la formation restreinte partage cette position.

27. La formation restreinte observe que, compte tenu de la responsabilité particulière de chacune des deux sociétés, la présidente de la Commission a décidé, le 24 juillet 2025, d'engager deux procédures de sanction autonomes à l'encontre des sociétés FREE MOBILE et FREE. Ainsi, les deux sociétés répondent chacune des obligations relatives à leur propre système d'information.

28. La formation restreinte relève que le rapport de sanction à l'encontre de la société FREE MOBILE fait état de manquements reprochés à cette dernière au regard du traitement relatif à la gestion des abonnés mobiles dont elle est seule responsable (ci-après dénommé traitement en cause). Il appartient à la formation restreinte d'examiner si les manquements allégués sont constitués et imputables à la société FREE MOBILE, conformément au principe de responsabilité personnelle.

29. La formation restreinte rappelle qu'elle n'entend pas se prononcer sur la survenance de la violation de données en tant que telle mais bien sur le fait de déterminer si, la société a ou non manqué à ses obligations de moyens au titre du RGPD, en qualité de responsable du traitement.

30. Par conséquent, la formation restreinte écarte l'argument de la société, qui considère que des manquements sont indistinctement reprochés par le rapporteur aux sociétés FREE MOBILE et FREE sur la base de mêmes constats, sans prise en compte de leurs responsabilités individuelles respectives.

B. Sur le manquement à l'obligation de conserver les données pour une durée proportionnée à la finalité du traitement en application de l'article 5-1-e) du RGPD

31. Aux termes de l'article 5, paragraphe 1, e) du RGPD, les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées […] .

32. En application de ces dispositions, il incombe au responsable de traitement de définir une durée de conservation conforme à la finalité du traitement. Lorsque cette finalité est atteinte, les données doivent être supprimées ou anonymisées, ou faire l'objet d'un archivage intermédiaire pour une durée déterminée lorsque leur conservation est nécessaire, par exemple pour le respect d'obligations légales ou à des fins précontentieuses ou contentieuses notamment.

33. A titre d'illustration, la délibération n° 2021-131 du 23 septembre 2021 portant adoption d'un référentiel relatif aux traitements mis en œuvre aux fins de gestion des activités commerciales recommande à des fins d'obligations comptables une durée de conservation, sous la forme d'archive intermédiaire, de dix ans.

34. Le rapporteur relève, qu'au jour du contrôle, la société n'avait pas mis en place de mesure permettant de trier les données des anciens abonnés qu'elle entendait conserver à des fins comptables durant dix ans. De plus, il souligne qu'une fois cette durée de dix ans atteinte, le mécanisme de purge des données n'était pas complètement opérationnel, de sorte que les données n'étaient jamais supprimées. La société conservait donc des données à caractère personnel de millions d'anciens abonnés pendant une durée excessive, ce qui constitue un manquement à l'article 5-1-e) du RGPD.

35. En défense, la société précise sa politique de durées de conservation des données.

36. Elle indique qu'afin de fournir ses produits et services, elle conserve les données à caractère personnel de ses abonnés pendant toute la durée du contrat. Elle précise que le terme contrat renvoie à la fois au contrat principal et aux contrats accessoires (par exemple, une ligne secondaire, la location de terminal mobile). Dès lors, elle conserve les données à caractère personnel de ses abonnés tant qu'un contrat (principal ou accessoire), dont ils sont titulaires, est en cours. Elle estime ainsi justifier la conservation des données de ses abonnés, qui ont résilié leur contrat principal, mais bénéficient toujours d'un contrat accessoire. Par exemple, les données d'identification, de facturation et de paiement restent nécessaires pour la gestion d'une location de terminal.

37. Par ailleurs, la société reconnaît avoir commis une erreur de déclaration lors du contrôle s'agissant de la durée de conservation des données à des fins de lutte contre la fraude. Elle précise conserver, à l'expiration du contrat, les données à caractère personnel de ses anciens abonnés pendant cinq ans, et non pas dix ans, à des fins de lutte contre la fraude.

38. En outre, elle indique conserver les données de ses abonnés pendant dix ans pour s'acquitter d'obligations comptables. La société soutient être tenue de conserver au titre des données de facturation, les données d'identification de l'abonné (nom, prénom, adresse), son identifiant client, le type d'offre souscrite, son IBAN et l'historique de ses règlements. Elle précise avoir lancé un projet afin de conserver uniquement les factures en format PDF, ce qui lui créera

des difficultés techniques dans son système d'information pour faire le lien entre une facture, un paiement et l'abonné concerné.

39. La société reconnaît qu'au jour du contrôle son mécanisme de purge des données n'était pas pleinement opérationnel, ce qu'elle justifie par des contraintes techniques. Elle ajoute qu'alors qu'elle a débuté son activité en 2012, la question de la suppression des données ne s'est posée que très récemment. Par ailleurs, l'architecture de son système d'information s'accorde difficilement avec des opérations de purge à grande échelle, compte tenu du risque de blocage des services métiers. Elle précise avoir débuté ce projet en 2023 afin de supprimer progressivement les données par lots (un premier lot en cours au jour du contrôle concernant les factures, suivi d'un second lot concernant les données des anciens abonnés qui devait être finalisé d'ici la fin d'année 2025). Elle soutient avoir conservé, au jour du contrôle, un nombre résiduel de données pendant une durée supérieure à dix ans et fait valoir avoir, au cours de la procédure, procédé à une purge manuelle de celles-ci.

40. Enfin, la société soutient que l'attaquant n'a pas accédé à des données à caractère personnel conservées pendant une durée excessive par la société dès lors que le compte usurpé ne permettait d'accéder qu'aux contrats en cours et à ceux résiliés depuis moins d'un an.

41. La formation restreinte relève que, si la politique de confidentialité de la société définit des durées de conservation différenciées en fonction des finalités poursuivies (notamment obligations comptables et lutte contre la fraude), les constatations réalisées au sein de la base de données de la société, associées aux déclarations de la société, démontrent l'absence de mise en œuvre effective de ces durées de conservation.

42. En effet, compte tenu du déploiement d'un mécanisme de purge qui n'était pas achevé au jour du contrôle, les données contenues dans la base de données de la société liées aux factures et aux abonnements résiliés étaient potentiellement conservées indéfiniment sans qu'aucune distinction ne soit faite en fonction des finalités poursuivies. La délégation de contrôle a ainsi constaté la présence de données (identifiant du compte, civilité, prénom, nom, adresse électronique et données contractuelles) relatives à plus de quinze millions de contrats résiliés depuis plus de cinq ans, dont trois millions depuis plus de dix ans.

43. Parmi ces trois millions de contrats pour lesquels les données étaient conservées depuis plus de dix ans, la société n'en justifie la conservation que pour 254 809 par l'existence d'autres contrats en cours d'exécution. Pour les 2 806 690 autres contrats, la société reconnait leur conservation pendant une durée excessive, qu'elle explique par des difficultés techniques liées à son mécanisme de purge alors en cours de déploiement.

44. La formation restreinte considère que ces difficultés ou défaillances techniques n'exonèrent pas la société de sa responsabilité de s'assurer du tri ou de la suppression des données aux échéances de leurs durées de conservation telles qu'elle les a elle-même définies.

45. La formation restreinte note que la société a indiqué, au cours de la procédure, avoir supprimé les données conservées depuis plus de dix ans à compter de la fin de la relation contractuelle, sans justification, à l'exception d'un reliquat de données relatives à 16 238 comptes, compte tenu de contraintes techniques. La société a indiqué que celui-ci sera supprimé d'ici la fin 2025.

46. Dès lors, la formation restreinte estime que la société a conservé, au jour du contrôle, des millions de données pendant une durée supérieure à dix ans, sans justification, ce qui est manifestement excessif.

47. S'agissant des données des contrats conservées pendant plus de cinq ans après la résiliation du contrat, la formation restreinte rappelle que la conservation de données au-delà de cette durée peut être justifiée pour une autre finalité que celle mentionnée par la société de lutte contre la fraude.

48. En effet, elle relève que la conservation de certaines données pendant une durée supérieure à cinq ans suivant la résiliation du contrat peut être justifiée par le respect de l'article L.123-22 du code de commerce, qui prévoit une obligation de conserver les données de facturation à des fins comptables pendant dix ans.

49. A l'issue des cinq années suivant la fin de la relation contractuelle, la société est dès lors tenue d'effectuer un tri, parmi toutes les données, afin de s'assurer de ne conserver que celles qui lui sont nécessaires à des fins comptables.

50. La formation restreinte note que la société a réalisé ce tri au cours de la procédure de sanction. Elle a décidé de conserver, pendant une durée supérieure à cinq ans suivant la résiliation du contrat, uniquement les factures au format PDF. La formation restreinte rappelle que la société n'est pas tenue de conserver les données de facturation uniquement en format PDF et peut les conserver, en format brut , dans sa base de données. Par ailleurs, la formation restreinte note que les données qui peuvent être conservées au titre de la facturation sont énumérées dans l'annexe de l'arrêté du 31 décembre 2013 relatif aux factures des services de communications électroniques et à l'information du consommateur sur la consommation au sein de son offre, et relève que celle-ci ne vise notamment pas les IBAN, de sorte que le tri réalisé en

cours de procédure par la société, qui inclut notamment l'IBAN comme une donnée à conserver, sans pour autant en avoir démontré l'utilité, n'est pas conforme au cadre réglementaire.

51. Ainsi, la formation restreinte considère, qu'au jour du contrôle, en conservant l'intégralité des données de ses anciens abonnés pendant plus de cinq ans après la résiliation du contrat, sans réaliser de tri pour s'assurer de ne conserver, pendant une durée plus longue, que celles qui étaient nécessaires à des fins de facturation, la société a conservé des données pendant une durée excessive.

52. Il résulte de ce qui précède que la formation restreinte considère qu'en conservant des données pendant des durées excessives la société a commis un manquement à l'article 5-1-e) du RGPD.

53. La formation restreinte note que la société a pris des mesures en cours de procédure, afin de supprimer certaines données à caractère personnel conservées pendant une durée excessive. Cependant, au jour de la séance, elle relève que la société ne démontre pas avoir procédé à la suppression des données relatives à 16 238 comptes résiliés depuis plus de dix ans. La société précise avoir prévu de lancer une purge en décembre 2025 afin de supprimer ces données. Par ailleurs, la société ne justifie pas, au jour de la séance, de la suppression des données qui ne lui sont pas strictement nécessaires à des fins comptables et qu'elle conservait, au jour du contrôle, pendant plus de cinq ans. La société précise que des mesures de mise en conformité sont en cours de déploiement et seront finalisées en juin 2026.

C. Sur le manquement à l'obligation d'assurer la sécurité des données en application de l'article 32 du RGPD

54. L'article 32, paragraphe 1, du RGPD dispose que compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque y compris entre autres, selon les besoins :

a) la pseudonymisation et le chiffrement des données à caractère personnel ;

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;

c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement […] .

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

1. La portée de l'obligation de sécurité prévue à l'article 32 du RGPD et la prévisibilité du cadre juridique applicable

56. La société soutient que l'obligation de sécurité prévue à l'article 32 du RGPD est une obligation de moyens et pas de résultat, de sorte que la survenance d'une violation de données ne saurait suffire à caractériser un manquement à cet article.

57. Par ailleurs, la société considère, compte tenu de l'absence de caractère prescriptif de l'article 32 du RGPD et de valeur contraignante des guides et recommandations de la CNIL et de l'ANSSI, que la formation restreinte ne peut pas caractériser un manquement à l'article 32 du RGPD sur le fondement d'instrument de droit souple sans violer le principe de légalité des délits et des peines, qui exige que la règle méconnue soit suffisamment claire et prévisible dans son application. Elle ajoute ne pas avoir pu bénéficier de précédents qui lui auraient permis d'apprécier la nature des mesures qui était attendues en ce qu'elle serait le premier organisme, victime d'un acte de malveillance extérieur, visé par une procédure de sanction de la CNIL sur le fondement de l'article 32 du RGPD.

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

59. Cette analyse a été confirmée par la CJUE dans son arrêt Agence nationale des recettes publiques de Bulgarie (14 décembre 2023, C/2024/1065, points 29 à 31). La formation restreinte relève que, dans cet arrêt, la CJUE a retenu que la référence, figurant à l'article 32, paragraphes 1 et 2, du RGPD, à un niveau de sécurité adapté au risque et à un niveau de sécurité approprié témoigne de ce que ce règlement instaure un régime de gestion des risques et qu'il ne prétend nullement éliminer les risques de violations des données à caractère personnel. Ainsi, il ressort des libellés des articles 24 et 32 du RGPD que ces dispositions se bornent à imposer au responsable du traitement d'adopter des mesures techniques et organisationnelles destinées à éviter, dans toute la mesure du possible, toute violation de données à caractère personnel. Le caractère approprié de telles mesures doit être évalué de manière concrète, en examinant si ces mesures ont été mises en œuvre par ce responsable en tenant compte des différents critères visés auxdits articles et des besoins de protection des données spécifiquement inhérents au traitement concerné ainsi qu'aux risques induits par ce dernier. Partant, les articles 24 et 32 du RGPD ne sauraient être compris en ce sens qu'une divulgation non autorisée de données à caractère personnel ou un accès non autorisé à de telles données par un tiers suffisent pour conclure que les mesures adoptées par le responsable du traitement concerné n'étaient pas appropriées, au sens de ces dispositions, sans même permettre à ce dernier d'apporter la preuve contraire.

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

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

62. La formation restreinte rappelle pouvoir sanctionner, non pas la survenance d'une violation de données, mais le fait que celle-ci a été rendue possible ou a été facilitée par l'absence ou l'insuffisance des mesures de sécurité mises en œuvre par un responsable du traitement, compte tenu de l'état de l'art. En ce sens, elle a déjà retenu, à plusieurs reprises, un manquement à l'article 32 du RGPD, compte tenu de l'absence ou de l'insuffisance des mesures de sécurité déployées qui a été exploitée par un attaquant dans le cadre d'une violation de données à caractère personnel (délibération n° SAN-2021-020 du 28 décembre 2021 § 61 ; délibération de la formation restreinte n° SAN-2020-014 du 7 décembre 2020 § 19 ; délibération de la formation restreinte n° SAN – 2019-005 du 28 mai 2019 § 31 ; délibération n° SAN-2018-011 du 19 décembre 2018). La formation restreinte considère que, bien que les mesures de sécurité visées dans ces précédents diffèrent du cas d'espèce, il n'en demeure pas moins que la société n'est pas la première visée par une procédure de sanction pour un manquement à l'article 32 du RGPD consécutif à une violation de données et qu'elle est responsable des mesures de sécurité qu'elle déploie pour assurer la protection des données qu'elle traite.

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

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

65. En second lieu, la formation restreinte relève que le principe de légalité des délits et des peines, rappelé par le Conseil constitutionnel en matière de sanction administrative (n° 88 - 248 DC, 17 janvier 1989), exige que les obligations et sanctions en cas de manquement aient été définis à l'avance.

66. Le Conseil d'État a précisé la portée de ce principe, qui implique que les éléments constitutifs des infractions soient définis de façon précise et complète (CE, 9 octobre 1996, Société Prigest, n° 170363, T. ; CE, Section, 12 octobre 2009, M. P., n° 311641, Rec.). En matière de sanctions administratives, la jurisprudence considère que l'exigence d'une définition des infractions sanctionnées se trouve satisfaite […] dès lors que les textes applicables font référence aux obligations auxquelles les intéressés sont soumis en raison de l'activité qu'ils exercent, de la profession à laquelle ils appartiennent, de l'institution dont ils relèvent ou de leur qualité et qu'une sanction peut être prononcé s'il est raisonnablement prévisible par les personnes concernées et en tenant compte de leur qualité et des responsabilités qu'elles exercent, que le comportement litigieux constitue un manquement à ces obligations (CE, 3 octobre 2018, SFCM, n° 411050, Rec.).

67. En l'espèce, la formation restreinte relève que, dans le cadre de ses écritures, le rapporteur s'attache notamment à caractériser la commission par la société d'un manquement aux obligations prévues à l'article 32 du RGPD, telles qu'éclairées par de nombreuses recommandations de la CNIL et de l'ANSSI, qui sont publiques et antérieures aux faits reprochés.

68. La formation restreinte rappelle que, si les recommandations de la Commission et de l'ANSSI n'ont certes pas de caractère impératif, elles précisent et illustrent les dispositions législatives et réglementaires applicables et éclairent les acteurs sur les mesures concrètes et conformes à l'état de l'art à mettre en œuvre.

69. Si c'est au seul regard des obligations prévues par l'article 32 du RGPD qu'un responsable de traitement peut être sanctionné, le Conseil d'Etat a néanmoins confirmé à plusieurs reprises que la formation restreinte de la CNIL pouvait retenir un manquement à l'article 32 du RGPD, caractérisé à la lumière de ses propres recommandations (CE, 11 mars 2015, Société Total Raffinage Marketing, n° 368748, n° 368819, pt 4 ; CE, 30 avril 2024, Commune de Beaucaire, n° 472864, pt 11).

70. Par conséquent, la formation restreinte relève que la société occupe une place significative dans le secteur des télécommunications en France et traite à ce titre les données de millions d'abonnés, et considère qu'elle dispose de moyens matériels, humains et techniques lui permettant d'assurer sa mise en conformité, d'adapter le cas échéant ses pratiques afin de respecter ses obligations au titre de l'article 32 du RGPD, telles qu'éclairées par les différentes recommandations de la CNIL et de l'ANSSI en matière de sécurité, qui existent depuis de nombreuses années.

71. Il résulte de ce qui précède que, dès lors que les éléments constitutifs du manquement à l'article 32 du RGPD reproché à la société sont définis de façon précise et complète, il ne peut être valablement soutenu que le prononcé d'une sanction méconnaîtrait le principe de légalité des délits et des peines.

72. La formation restreinte écarte donc le grief tiré de la méconnaissance du principe de légalité des délits et des peines.

2. Sur les risques du traitement pour les personnes concernées

73. Le rapporteur rappelle que la société doit assurer un niveau de sécurité, à l'égard des données à caractère personnel qu'elle traite, qui s'apprécie au regard des risques liés à la divulgation et à l'accès non autorisé de celles-ci, compte tenu des conséquences que pourrait avoir la survenance de tels risques pour les personnes concernées. En l'espèce, il souligne le caractère massif du traitement (données d'environ 15,5 millions d'abonnés mobiles et certaines données détenues par la société FREE en cas de clients convergents), ainsi que le caractère hautement personnel de certaines données (données bancaires), ce qui présente de forts risques pour les personnes concernées en cas d'atteinte à la confidentialité de ces données (usurpation de leur identité, tentative d'hameçonnage et exploitation frauduleuse de leurs coordonnées bancaires).

74. La société estime que le traitement qu'elle met en œuvre ne présente pas de risque élevé pour les personnes concernées en l'absence de données sensibles au sens de l'article 9 du RGPD.

75. Par ailleurs, elle soutient que la compromission des IBAN n'entraîne pas de risque particulier dès lors qu'un IBAN seul ne permet pas de réaliser un prélèvement frauduleux et que les établissements bancaires ont mis en place des mécanismes pour l'éviter (nécessité d'obtenir la signature d'un mandat SEPA avant tout prélèvement, délai de contestation et remboursement en cas de fraude).

76. En outre, la société estime que la recrudescence de violations de données ne permet pas d'imputer le préjudice allégué par certains plaignants (hameçonnage, etc.) à l'attaque dont elle a été victime, qui n'a dans ce contexte pas créé de risque supplémentaire pour les personnes concernées.

77. La formation restreinte rappelle que le considérant 75 du RGPD vise des risques pour les droits et libertés des personnes physiques, dont le degré de probabilité et de gravité varie, peuvent résulter du traitement de données à caractère personnel qui est susceptible d'entraîner des dommages physiques, matériels ou un préjudice moral, en particulier: lorsque le traitement peut donner lieu […] à un vol ou une usurpation d'identité, à une perte financière, […] ou lorsque le traitement porte sur un volume important de données à caractère personnel et touche un nombre important de personnes concernées .

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

79. Par ailleurs, le considérant 83 du RGPD précise que dans le cadre de l'évaluation des risques pour la sécurité des données, il convient de prendre en compte les risques que présente le traitement de données à caractère personnel, tels que la destruction, la perte ou l'altération, la divulgation non autorisée de données à caractère personnel transmises,

conservées ou traitées d'une autre manière ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite, qui sont susceptibles d'entraîner des dommages physiques, matériels ou un préjudice moral .

80. En l'espèce, le traitement relatif à la gestion des abonnés au moyen de l'outil MOBO permet à la société d'accéder aux données de chacun de ses abonnés contenus dans sa propre base de données mobile, mais également d'accéder, en cas de clients convergents (clients à la fois de la société FREE MOBILE et de la société FREE), aux données contenues dans la base de données des abonnés fixes de la société FREE, notamment l'IBAN. Au jour de la violation de données, l'outil métier de la société FREE MOBILE permettait, lorsqu'un salarié réalisait une recherche, de renvoyer l'entièreté de l'IBAN des clients convergents présents dans la base de données fixe de la société FREE, compte tenu d'une anomalie technique survenue lors d'une mise à jour de cet outil, corrigée après la prise de connaissance de la violation de données par la société FREE MOBILE.

81. Au 31 décembre 2024, la société FREE MOBILE comptait environ 15,5 millions d'abonnés mobiles et la société FREE environ 7,6 millions d'abonnés fixes.

82. La formation restreinte considère que l'accès non autorisé ou la divulgation des données traitées par la société est de nature à créer un préjudice moral et matériel pour les personnes concernées. En effet, comme relevé par la société dans le cadre de ses notifications auprès de la CNIL, celles-ci sont exposées à des risques liés à la revente de leurs données à des personnes malveillantes, une usurpation de leur identité, des tentatives d'hameçonnage (pratique consistant, pour une personne malveillante, à se faire passer pour un organisme connu de la personne concernée afin par exemple de lui demander ses coordonnées bancaires). La formation restreinte relève que le rapporteur démontre, dans ses écritures, l'existence d'un risque de paiements frauduleux au moyen d'un IBAN usurpé. En effet, une personne mal intentionnée, disposant d'un IBAN usurpé, peut procéder à un paiement frauduleux sur un site web qui propose de valider le mandat de prélèvement SEPA par l'intermédiaire d'une simple case à cocher.

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

84. En ce sens, la formation restreinte observe qu'un certain nombre de plaignants ont fait état auprès de la Commission d'utilisations frauduleuses de leurs données à la suite de la violation de données en cause, notamment des tentatives d'hameçonnage. S'il n'est pas possible de déterminer avec certitude que les fraudeurs ont obtenu les données des plaignants par la violation de données en cause, et non par celle subie par un tiers disposant des mêmes données, il est constant que la perte de confidentialité des données traitées par FREE MOBILE a participé à l'augmentation du volume de données disponibles pour les attaquants potentiels. L'existence d'autres violations de données n'est en tout état de cause pas de nature à décharger la société de son obligation de mettre en œuvre les mesures de sécurité adaptées au risque de compromission des données qu'elle traite.

85. La formation restreinte considère que les mesures de sécurité mises en place par la société FREE MOBILE auraient dû permettre de répondre aux risques qui viennent d'être exposés.

3. Sur le niveau de sécurité déployé par la société

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

En l'espèce, la formation restreinte va devoir analyser si la société a mis en place un ensemble cohérent de mesures de sécurité pour protéger son système d'information.

3.1 Sur les vulnérabilités ayant conduit ou facilité la survenance de la violation de données en cause

3.1.1 Sur l'absence de sécurisation du canal d'interconnexion

87. Dans un contexte numérique, il est possible pour un salarié de se connecter à distance (par exemple, depuis son domicile) au système d'information de sa société au moyen de son ordinateur portable. Il s'agit de nomadisme numérique.

88. L'ANSSI définit le nomadisme numérique comme toute forme d'utilisation des technologies de l'information permettant à un utilisateur d'accéder au SI [système d'information] de son entité d'appartenance ou d'emploi, depuis des lieux distants, ces lieux n'étant pas maîtrisés par l'entité (ANSSI, Recommandations sur le nomadisme numérique , 2018).

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

90. Ainsi, l'ANSSI souligne que dans le cadre du nomadisme, l'objectif est de réussir à s'aligner avec le niveau de sécurité du SI [système d'information] interne de l'entité, en répondant aux risques d'exposition plus forts listés ci-dessus .

91. Elle considère que les entités doivent adopter des mesures spécifiques au nomadisme dans leurs politiques de sécurité du système d'information afin de réduire ou de couvrir les risques susvisés.

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

93. L'ANSSI rappelle qu' en fonction des moyens d'authentification mis en œuvre sur le poste nomade, un attaquant peut tenter d'usurper l'identité de l'utilisateur ou celle du poste nomade . Dès lors, il est important d'utiliser des mécanismes robustes […] d'authentification […] pour la mise en place du canal d'interconnexion d'un poste nomade .

94. En situation de nomadisme, l'ANSSI estime que trois niveaux d'authentification doivent être considérés :

- authentification de l'utilisateur sur le poste nomade ;

- authentification du poste nomade sur le SI [système d'information] ;

- authentification de l'utilisateur sur le SI [système d'information] .

95. S'agissant plus spécifiquement de l'authentification du poste nomade sur le système d'information de l'entité, l'ANSSI rappelle que l'objectif est de garantir que le poste utilisé pour accéder au système d'information est un équipement maîtrisé par l'entité afin de réduire les risques qui résulteraient de l'utilisation de postes nomades non maîtrisés et dont le niveau de sécurité ne serait pas conforme à la politique de sécurité de l'entité. Elle recommande d'authentifier le poste nomade sur le SI [système d'information] au moyen d'un certificat machine [c'est-à-dire d'un certificat lié au poste nomade et non pas à l'utilisateur du poste nomade] et de protéger la clé privée de ce certificat en intégrité et en confidentialité, afin de s'assurer qu'elle ne puisse être accédée ni par l'utilisateur nomade ni par un attaquant .

96. Dès lors, l'ANSSI recommande depuis 2018 d'authentifier le poste nomade d'un utilisateur sur un système d'information au moyen d'un certificat machine, qui est lié au poste nomade et non pas à l'utilisateur de celui-ci.

97. Dans son Guide de la sécurité des données personnelles de mars 2024, la CNIL recommande également de privilégier l'authentification multi facteur lorsque cela est possible, en particulier lorsque la connexion est accessible depuis l'extérieur du réseau de l'organisme .

98. Il résulte de ce qui précède que tant l'ANSSI que la CNIL recommandent d'authentifier un utilisateur sur un système d'information en mettant en œuvre une authentification multi facteur forte, notamment lorsque la connexion au système d'information de l'entité est accessible depuis l'extérieur de son réseau.

99. Le rapporteur reproche à la société de ne pas avoir mis en place des mesures de sécurité appropriées pour sécuriser l'accès par les utilisateurs au VPN de la société, à savoir une authentification des postes nomades et une authentification multi facteur des utilisateurs. Il considère que ces vulnérabilités constituent un manquement à l'article 32 du RGPD et ont rendu possible ou a minima facilité la survenance de la violation de millions de données à caractère personnel d'abonnés de la société entre le 28 septembre et le 22 octobre 2024. Il note que la société a entamé le déploiement de ces mesures au cours de la procédure de sanction afin de se mettre en conformité.

100. En défense, la société soutient avoir mis en place, au jour du contrôle, des mesures de sécurité suffisamment robustes s'agissant de l'authentification des utilisateurs et de leurs postes lors de leur connexion à son VPN.

101. […].

102. […].

103. […].

104. […].

105. […].

106. A titre liminaire, la formation restreinte rappelle que dans le contexte de nomadisme numérique, il revient au responsable de traitement de déployer des mesures permettant de garantir que, tant la personne qui se connecte, que la machine qu'elle utilise, bénéficient des autorisations nécessaires pour se connecter aux ressources internes. Ces mesures s'ajoutent à celles qui doivent exister lorsqu'une personne est déjà authentifiée sur le réseau, telles que des mécanismes d'authentification robustes lors de l'accès à des outils.

107. […].

108. La formation restreinte rappelle que la connexion au VPN d'une entité par des postes qui n'appartiennent pas à son parc informatique présente un risque pour son système d'information dès lors qu'elle ne maîtrise pas les mesures de sécurité mises en œuvre sur ces équipements, qui peuvent donc ne pas correspondre au niveau de sécurité défini dans sa politique interne.

109. […].

110. […].

111. […].

112. […].

113. […].

114. […].

115. […].

116. […].

117. […].

118. […].

3.1.2 Sur l'absence de détection des comportements anormaux

119. Dans sa délibération n° 2021-122 du 14 octobre 202 portant adoption d'une recommandation relative à la journalisation, la CNIL rappelle que la mise en place d'un dispositif de journalisation participe au respect de l'obligation de sécurisation de tout traitement de données à caractère personnel, en application des articles 5 et 32 du RGPD .

120. Ainsi, elle recommande aux organismes de collecter des informations sur les personnes administrant ou accédant à leurs ressources, comme l'identifiant de l'utilisateur, la date et l'heure de l'accès et l'identifiant de l'équipement utilisé (CNIL, La CNIL publie une recommandation relative aux mesures de journalisation , 18 novembre 2021).

121. La CNIL rappelle dans sa recommandation susvisée que cette sécurisation est essentiellement active : elle repose sur une exploitation en temps réel ou à court terme de ces données pour détecter des opérations anormales afin de parer des attaques ou intrusions, ou de remédier rapidement à un incident informatique en facilitant l'identification du problème .

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

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

124. La Commission recommande donc, dans sa recommandation susvisée, de mettre en œuvre un système de traitement et d'analyse des données collectées et de formaliser un processus permettant de générer des alertes et de les traiter en cas de suspicion de comportement anormal. Ces données peuvent également servir ex post lorsqu'une violation de données (notamment par consultation, transmission ou usage illégaux des données) est constatée et que le responsable de traitement cherche à en établir la responsabilité .

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

126. Le rapporteur considère, qu'au jour du contrôle, les mesures de sécurité mises en œuvre par la société pour détecter une activité suspecte sur son VPN, son réseau interne et son outil de gestion de clientèle MOBO étaient insuffisantes, ce qui a rendu possible, ou a minima facilité, la perte de confidentialité de millions de données à caractère personnel d'abonnés de la société entre le 28 septembre et le 22 octobre 2024. Il note que la société s'est toutefois mise en conformité sur ce point au cours de la procédure.

127. En premier lieu, la société soutient, s'agissant des moyens de détection des connexions frauduleuses à son VPN, avoir déployé des mesures suffisamment robustes au jour du contrôle.

128. Elle indique qu'elle recourait déjà à la solution de scoring […] proposée par un prestataire externe. Il s'agit d'une solution de prévention de la fraude, d'analyse des risques et de détection des menaces. Elle produit des indicateurs pour chacune des connexions à son VPN, à partir de plusieurs critères (par exemple, la localisation de l'adresse IP, ou le fait que l'utilisateur se connecte au VPN de la société via un VPN tiers) et attribue notamment un score de fraude entre 0 et 100 afin d'évaluer son niveau de risque (de faible à maximal). La société exploite les indicateurs générés par la solution […] afin de décider d'autoriser ou de refuser des connexions à son VPN.

129. La société indique, qu'à l'issue du contrôle, elle a déployé un centre opérationnel de sécurité qui assure une surveillance continue notamment des connexions à son VPN et mis en place une équipe interne dédiée aux réponses aux incidents de sécurité informatique.

130. En deuxième lieu, s'agissant des moyens de détection des comportements suspects sur son réseau interne, la société indique avoir déployé, à la suite du contrôle, un système de surveillance des flux de données circulant sur son réseau.

131. En troisième lieu, s'agissant des moyens de détection des comportements anormaux sur l'outil MOBO, la société considère avoir, au jour du contrôle, mis en œuvre des mesures de sécurité suffisantes en déployant un dispositif de journalisation uniquement pour la fonctionnalité consultation , qui est la seule fonction permettant d'accéder de manière effective aux données de ses abonnés. Elle estime qu'il n'était pas nécessaire de déployer un mécanisme de surveillance et de détection pour la fonctionnalité recherche de son outil dès lors que celle-ci ne permet pas d'accéder à des données à caractère personnel. Elle précise que lorsqu'un utilisateur effectue une recherche et que celle-ci renvoie plusieurs résultats, l'utilisateur doit, pour accéder aux données des abonnés, cliquer sur la fonction consultation . Elle ajoute que lorsqu'une recherche renvoie un seul résultat, la fonctionnalité consultation , qui fait l'objet d'une surveillance, est automatiquement appelée.

132. Compte tenu de la position du rapporteur, la société indique avoir pris de nouvelles mesures de sécurité en instaurant un dispositif de surveillance des fonctions de recherches et de consultation de son outil MOBO avec un blocage automatique en fonction de certains critères et mis en place un tableau de bord de suivi notamment des utilisateurs bloqués, et des volumes de recherches par profil utilisateur.

133. En premier lieu, la formation restreinte relève, s'agissant des moyens de détection des connexions frauduleuses à son VPN, qu'il ressort des éléments communiqués par la société que celle-ci dispose d'un dispositif d'évaluation des connexions à son VPN et qu'elle l'a paramétré afin d'accepter, par défaut, l'ensemble des connexions à son VPN, sauf dans deux cas.

134. […].

135. […]:

136. […].

137. […].

138. […].

139. […].

140. […].

141. […].

142. […].

143. La formation restreinte observe que le dispositif d'analyse des connexions s'est donc avéré inefficace face à l'attaque alors même que le nombre anormal de connexions à son système d'information, qui ne correspondait aucunement à un usage standard, constituait un indicateur à prendre en compter afin de déterminer leur légitimité. Cette vulnérabilité a notamment été exploitée par l'attaquant dans le cadre de la violation de données en cause. En effet, en l'absence de détection de son intrusion dans le système d'information de la société, il a été en mesure d'accéder, pendant presque un mois, à de très nombreuses reprises, aux données à caractère personnel qu'il contient, sans être arrêté par la société.

144. Il en résulte que les mesures mises en œuvre par la société pour détecter les connexions frauduleuses à son VPN étaient insuffisantes au jour du contrôle.

145. De surcroit, la formation restreinte relève qu'au jour du contrôle, la société n'avait pas non plus déployé de mesures suffisantes permettant de détecter les comportements suspects sur son réseau interne. Dès lors, la société ne détectait ni les connexions frauduleuses à son VPN ni l'intrusion dans son réseau interne. Ainsi, lors de l'attaque, une fois connecté au VPN, l'attaquant a pu accéder au réseau interne de la société, et donc à ses ressources, sans être détecté. L'absence de système d'alerte relatif au trafic sur le réseau interne de la société est donc également une vulnérabilité utilisée par l'attaquant et a ainsi favorisé la violation de données.

146. En deuxième lieu, s'agissant des moyens de détection des comportements anormaux sur l'outil MOBO, la formation restreinte rappelle que cet outil propose à ses utilisateurs de remplir un formulaire afin de réaliser une recherche concernant un abonné de la société, et d'accéder aux résultats de cette recherche par l'intermédiaire d'une fonctionnalité de consultation . La formation restreinte relève que les fonctions recherche et consultation font toutes les deux l'objet d'une journalisation mais, qu'au jour du contrôle, seule la fonctionnalité consultation était analysée par un système créant des alertes en cas d'utilisation anormale.

147. La formation restreinte observe que la fonctionnalité recherche de l'outil MOBO ne permet pas à un utilisateur d'afficher directement sur son écran les résultats des recherches effectuées et donc les données à caractère personnel qu'ils contiennent. En effet, soit les résultats de la recherche comportent plusieurs résultats et l'utilisateur doit cliquer sur la fiche d'un abonné pour accéder à la consultation des données, soit les résultats de la recherche comportent un seul résultat et les données sont affichées grâce au déclenchement de la fonctionnalité consultation .

148. La formation restreinte observe toutefois que lorsqu'un utilisateur réalise une recherche , l'outil MOBO renvoie une réponse http dont le contenu est accessible, sans passer par la fonction consultation . En effet, en ouvrant l'outil de développement du navigateur, l'utilisateur peut accéder aux résultats de la recherche, celles-ci comportant les données à caractère personnel de l'abonné.

149. Dès lors, la formation restreinte considère que les requêtes, qui permettaient de prendre connaissance des résultats de la recherche et donc d'accéder aux données à caractère personnel, auraient également dû faire l'objet d'une analyse de journalisation, de la même manière que la fonctionnalité consultation .

150. La formation restreinte souligne que cette vulnérabilité a été exploitée par l'attaquant dans le cadre de la violation de données en cause. […].

151. Au regard de l'ensemble de ces éléments, la formation restreinte considère, qu'au jour du contrôle, la société n'avait pas déployé les moyens suffisants pour être en mesure de détecter les activités suspectes sur son VPN, son réseau interne et son outil de gestion de ses abonnés, ce qui constitue un manquement à l'article 32 du RGPD.

152. La formation restreinte relève que la société a pris des mesures au cours de la procédure permettant de mettre fin au manquement constaté. Elle considère, dès lors, qu'il n'y a pas lieu de prononcer une injonction de mise en conformité, comme initialement proposé par le rapporteur.

3.2 Sur l'absence de robustesse liée au stockage des mots de passe des utilisateurs de l'outil MOBO

153. La conservation des mots de passe de manière sécurisée constitue une précaution élémentaire en matière de protection des données à caractère personnel. Dès 2013, l'ANSSI alertait et rappelait les bonnes pratiques s'agissant de la conservation des mots de passe en indiquant que ces derniers doivent être stockés sous une forme transformée par une fonction cryptographique à sens unique (fonction de hachage) et lente à calculer telle que PBKDF2 et que la transformation des mots de passe doit faire intervenir un sel aléatoire pour empêcher une attaque par tables précalculées (ANSSI, Bulletin d'actualité CERTA-2013-ACT-046 , 15 novembre 2013, https://www.cert.ssi.gouv.fr/actualite/CERTA-2013-

ACT-046/). L'ANSSI précisait également dans ses recommandations relatives à l'authentification multi facteur et aux mots de passe que les fonctions de hachage cryptographique recommandées, comme la famille SHA2, sont des fonctions très rapides à exécuter, ce qui, dans le contexte du stockage des mots de passe, est un avantage pour les attaquants, leur permettant de tester de nombreux mots de passe (https://cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe).

154. De même, dans sa délibération n° 2017-012 du 19 janvier 2017, la CNIL indiquait déjà qu'elle recommande [que le mot de passe] soit transformé au moyen d'une fonction cryptographique non réversible et sûre (c'est-à-dire utilisant un algorithme public réputé fort dont la mise en œuvre logicielle est exempte de vulnérabilité connue), intégrant l'utilisation d'un sel ou d'une clé , recommandation confirmée dans sa délibération n°2022-100 du 21 juillet 2022. En effet, les fonctions de hachage non robustes présentent des vulnérabilités connues qui ne permettent pas de garantir l'intégrité et la confidentialité des mots de passe en cas d'attaque par force brute après compromission des serveurs qui les hébergent. La CNIL recommande également, dans son Guide RGPD du développeur publié le 27 janvier 2020, que le stockage d'un mot de passe se fasse au moyen d'une librairie éprouvée, comme Argon2, yescrypt, scrypt, balloon, bcrypt et, dans une moindre mesure, PBKDF2 .

155. Ainsi, le stockage des mots de passe des utilisateurs doit être réalisé de façon sécurisée. A cet égard, il est recommandé de stocker les empreintes de mots de passe plutôt que les mots de passe en clair. Pour obtenir une telle empreinte de mot de passe, il est en principe nécessaire de recourir à une fonction de hachage cryptographique mathématiquement éprouvée et lente à exécuter, tout en utilisant un sel aléatoire et long pour chaque mot de passe (d'une longueur d'au moins 128 bits), et ce, afin de se prémunir contre des attaquants qui auraient précalculé des tables de correspondance entre les mots de passe et leurs empreintes respectives.

156. […].

157. […].

158. A titre liminaire, la formation restreinte rappelle que, dans le cadre de la violation de données en cause, l'attaquant n'a pas exploité de vulnérabilité liée aux modalités de stockage des mots de passe des utilisateurs de l'outil MOBO.

159. […].

160. […].

161. […].

162. Par conséquent, la formation restreinte considère qu'il revenait à la société FREE MOBILE d'utiliser un algorithme de stockage de mot de passe lent et coûteux en espace mémoire, tel que cela ressort clairement des recommandations de l'ANSSI et de la CNIL précitées, afin de permettre en cas d'attaque, par exemple par force brute ou par dictionnaire, de ralentir un attaquant dans son identification des mots de passe.

163. La formation restreinte considère que les modalités de stockage des mots de passe des utilisateurs de l'outil MOBO constitue une vulnérabilité du système d'information de la société, peu important que celle-ci ait été exploitée ou non par l'attaquant dans le cadre de la violation de données en cause.

164. […].

165. Au vu de ce qui précède, la formation restreinte considère, qu'au jour du contrôle, les modalités de stockage des mots de passe des utilisateurs de l'outil MOBO ne permettaient pas d'assurer leur confidentialité, ce qui constitue un manquement aux dispositions de l'article 32 du RGPD.

166. […].

D. Sur le manquement à l'obligation de communiquer aux personnes concernées de la survenance d'une violation de données à caractère personnel en application de l'article 34 du RGPD

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

168. Le paragraphe 2 de l'article susmentionné précise les mentions qui doivent obligatoirement figurer dans le contenu de cette communication. Celle-ci doit contenir une description de la nature de la violation de données, des conséquences probables de la violation de données à caractère personnel, ainsi que des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives. Par ailleurs, elle doit communiquer le nom et les

coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenue.

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

170. Le rapporteur considère que la société a commis un manquement à l'article 34 du RGPD dès lors que le courriel d'information adressé par la société aux personnes concernées par la violation de données ne permet de les éclairer ni quant aux mesures de remédiation qu'elle a prises, ni sur les conséquences probables de la violation de données, ni enfin sur les mesures que ces personnes doivent prendre pour se prémunir des risques auxquels la violation les expose.

171. En défense, la société estime avoir respecté l'article 34 du RGPD.

172. Tout d'abord, sur la forme de la communication, la société indique avoir adopté une approche à plusieurs niveaux. D'une part, un courriel a été adressé aux personnes concernées, entre les 24 et 29 octobre 2024, afin de leur communiquer un premier niveau d'information synthétique. La société précise avoir procédé à une communication échelonnée afin d'éviter de saturer les serveurs de messagerie des personnes. D'autre part, un second niveau d'information a été communiqué aux personnes par l'intermédiaire d'un numéro vert gratuit disponible 7 jours sur 7, visé dans le courriel d'information initial, et d'un dispositif interne de gestion des demandes (ticket DPO). La société précise que le numéro vert mis en place lui a permis de répondre à 58 239 appels et que, grâce au système de ticket DPO, elle a pu traiter 1 081 demandes.

173. Puis, sur le fond de la communication, la société considère que le courriel d'information initial était complet au regard des exigences posées par l'article 34, paragraphe 2, du RGPD. Elle fait valoir que celui-ci informait les personnes de la survenance de la violation de données en cause, les alertait sur les risques de courriels, SMS ou appels frauduleux , leur rappelait que ses conseillers ne demandent jamais la communication de mots de passe à l'oral et elle les invitait, en cas de situation anormale, à consulter le site officiel cybermalveillance.gouv.fr pour effectuer un signalement.

174. La société justifie l'envoi d'un message de vigilance générale par le fait qu'elle ne pouvait pas anticiper toutes les formes d'exploitation futures de la violation de données.

175. Plus spécifiquement la société soutient que l'article 34, paragraphe 2, du RGPD, qui renvoie à l'article 33, paragraphe 3, ne lui imposait pas de détailler aux personnes concernées l'ensemble des mesures prises afin de mettre fin à la violation de données. Elle considère qu'une position contraire engendrerait un risque de compromission de la sécurité du système d'information concerné.

176. Enfin, la société considère que le nombre important de plaintes reçues par la CNIL résulte de la médiatisation exceptionnelle de la violation de données, à laquelle la CNIL a participé. Elle considère que les fraudes et tentatives de fraude, dont font état certains plaignants, ne sont pas imputables à un défaut d'informations de sa part dès lors qu'elle a pris les mesures nécessaires pour sensibiliser ses abonnés aux risques de fraude (notamment, par la mise en ligne d'une page d'assistance dédiée au phishing, une campagne de sensibilisation par courriel, la mise en place d'une veille proactive des sites susceptibles de conduire des campagnes de phishing visant ses abonnés).

177. La formation restreinte rappelle que l'article 34 du RGPD impose à un responsable de traitement, victime d'une violation de données, de communiquer certaines informations aux personnes concernées lorsque la violation de données est susceptible d'engendrer un risque élevé pour leurs droits et libertés.

178. La formation restreinte rappelle également que, comme le souligne le Comité européen de la protection des données (ci-après CEPD) dans ses lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679 adoptées le 28 mars 2023, l'objectif principal [de l'article 34 du RGPD] est d'aider les personnes concernées à comprendre la nature de la violation ainsi que les mesures qu'elles peuvent mettre en place pour se protéger .

179. Ainsi, le paragraphe 2 de l'article 34 du RGPD prévoit que la communication aux personnes concernées doit décrire la nature de la violation de données à caractère personnel et contenir au moins les informations et mesures mentionnées à l'article 33, paragraphe 3, points b), c) et d). Ces informations concernent le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues (point b), la description des conséquences probables de la violation de données à caractère personnel (point c), et la description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives (point d).

180. La formation restreinte considère qu'il résulte de la rédaction du paragraphe 2 de l'article 34 du RGPD que les informations énumérées ci-dessus sont celles qui doivent, a minima, être communiquées aux personnes concernées par une violation de données à caractère personnel lorsque celle-ci est susceptible d'engendrer un risque élevé pour leurs droits et libertés.

181. Dès lors, ces informations doivent être adressées directement aux personnes concernées, dans un premier niveau d'information, car elles sont essentielles pour atteindre l'objectif poursuivi par la communication : leur permettre de comprendre la nature de la violation, ainsi que les mesures qu'elles peuvent mettre en place pour se protéger.

182. Par ailleurs, la formation restreinte observe que l'obligation, pour un responsable de traitement, de communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact , comme prévu par le point b) du paragraphe 2 de l'article 33 du RGPD, a pour objectif de fournir aux personnes concernées par la violation de données des informations supplémentaires . La formation restreinte estime que ces informations viennent donc compléter les informations essentielles devant figurer dans le premier niveau d'information et ne sauraient s'y substituer.

183. En ce sens, la formation restreinte relève que, dans ses lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE)2016/679 adoptées le 28 mars 2023, le CEPD rappelle qu' un responsable du traitement peut choisir de fournir des informations complémentaires à celles présentées ici [article 33, paragraphe 3, points b), c) et d)] comme nécessaires .

184. Autrement dit, l'article 34, paragraphe 2, du RGPD, qui renvoie à son article 33, paragraphe 3, point b), prévoit la possibilité de communiquer auprès des personnes concernées à deux niveaux d'information : un premier, obligatoire, comportant les informations essentielles et un second comportant des informations complémentaires que le responsable du traitement souhaite porter à la connaissance des personnes.

185. En l'espèce, en premier lieu, la formation restreinte relève que la société a adressé aux personnes concernées par la violation de données un premier courriel d'information, qui constitue un premier niveau d'information. La société a, par ailleurs, mis en place un numéro vert gratuit, accessible 7 jours sur 7, de 9 heures à 18 heures, dont elle communique les coordonnées dans son courriel initial, ainsi qu'un système de ticket DPO , pour répondre aux questions complémentaires des personnes, qui constitue un second niveau d'information.

186. La formation restreinte considère que la forme de la communication réalisée à destination des personnes concernées est conforme aux exigences posées par l'article 34, paragraphe 2, du RGPD.

187. En deuxième lieu, la formation restreinte relève que le courriel adressé aux personnes concernées les informait du fait que la société avait été victime d'une cyberattaque ciblant son outil de gestion, ayant entraîné un accès non autorisé à une partie des données à caractère personnel associées aux comptes des abonnés (leurs nom, prénom, adresse électronique, adresse postale, date et lieu de naissance, numéro de téléphone, identifiant abonné et données contractuelles). Ce courriel précisait également que toutes les mesures nécessaires ont été prises immédiatement pour mettre fin à cette attaque et renforcer la protection de [ses] systèmes d'information , que la violation de données avait été notifiée à la CNIL, ainsi qu'à l'ANSSI, et qu'une plainte avait également été déposée auprès du procureur de la République. En outre, la société invitait les personnes concernées à la plus grande vigilance face au risque d'emails, SMS ou appels frauduleux , précisait que ses conseillers ne demandaient jamais la communication à l'oral de mot de passe et les invitait, en cas de suspicion ou de situation anormale à contacter le service officiel d'assistance aux victimes numériques sur le site web cybermalveillance.gouv.fr afin d'effectuer un signalement. Enfin, pour toute question et demande de renseignement , le courriel précisait que la société tenait à la disposition des personnes concernées un numéro vert, gratuit, accessible 7 jours sur 7, de 9 heures à 18 heures.

188. La formation restreinte estime que, si la majorité des informations essentielles figuraient dans le courriel d'information initial et que le mode de communication permettait aux personnes concernées d'accéder aux autres informations essentielles par l'intermédiaire du second niveau d'information, il n'en demeure pas moins que certains éléments importants n'étaient pas mentionnés.

189. S'agissant de l'information relative aux mesures de remédiation, il est admis que, dans certains cas, des mesures de sécurité déployées par un organisme doivent effectivement rester secrètes afin de ne pas exposer son système d'information à des risques de nouvelles attaques. La formation restreinte précise, cependant, que toutes les mesures de sécurité mises en œuvre par un organisme ne présentent pas un risque pour la sécurité d'un système d'information et n'ont donc pas nécessairement vocation à demeurer secrètes.

190. La formation restreinte observe que la société a uniquement indiqué aux personnes concernées par la violation de données en cause que toutes les mesures nécessaires ont été prises immédiatement pour mettre fin à cette attaque et renforcer la protection de nos systèmes d'information , ce qui constitue, selon la formation restreinte, une formulation trop générale et abstraite pour se conformer à l'article 34, paragraphe 2, du RGPD. En effet, l'article 33, paragraphe 3, point d), auquel l'article susmentionné renvoie, prévoit une obligation de décrire ces mesures.

191. La formation restreinte estime dès lors que, sans mettre en danger son système d'information, la société aurait dû décrire , même brièvement, dans des termes simples, les principales mesures correctives qu'elle avait prises pour remédier à la violation de données en cause. La formation restreinte rappelle que l'objectif de cette communication est de rassurer les personnes concernées sur la protection effective de leurs données à caractère personnel.

192. La formation restreinte relève que, dans le cadre de la notification initiale effectuée auprès de la CNIL quelques jours avant la communication réalisée auprès des personnes concernées, la société avait bien décrit ces mesures, conformément à l'article 33 du RGPD (obligation de notifier la violation de données à la Commission). Sans entrer dans le détail de ces mesures pour permettre la lisibilité de la communication aux personnes, la formation restreinte considère que la société aurait notamment dû indiquer avoir procédé à la révocation des accès compromis, à la correction de vulnérabilités liées à son outil métier, et au renforcement des contrôles des accès aux données à caractère personnel. Ces éléments d'information sont compréhensibles pour les personnes concernées et ne sont pas de nature à compromettre le système d'information de la société.

193. S'agissant de l'information relative aux conséquences probables de la violation de données en cause et des mesures à prendre pour en atténuer les éventuelles conséquences négatives, la formation restreinte rappelle que la société a indiqué aux personnes concernées nous vous invitons à la plus grande vigilance face au risque d'emails, SMS ou appels frauduleux. Sachez que nos conseillers ne vous demanderont jamais vos mots de passe à l'oral. En cas de suspicion ou de situation anormales, nous vous invitons à contacter le service officiel d'assistance aux victimes numériques sur : www.cybermalveillance.gouv.fr pour effectuer un signalement et faire valoir vos droits .

194. La formation restreinte estime que cette formulation est trop vague pour atteindre l'objectif d'aider les personnes concernées à comprendre les principaux risques auxquels elles sont exposées, ainsi que les mesures qu'elles peuvent mettre en place pour s'en protéger.

195. En effet, d'une part, la formation restreinte considère que les personnes concernées ne sont pas mises en mesure d'appréhender le contexte dans lequel elles pourraient être sollicitées par courriel, SMS ou téléphone, ni de comprendre les réflexes à adopter pour se prémunir des conséquences négatives. La formation restreinte observe que la société avait pourtant bien identifié, dans le cadre des scripts de questions/réponses mis à la disposition des conseillers répondant aux appels, qu'il existait un scénario de risque relatif à des tentatives de fraude en se faisant passer pour Free ou tout autre organisme . La formation restreinte note qu'elle avait également identifié des recommandations à prodiguer aux personnes (par exemple : ne jamais communiquer ses informations personnelles par email, SMS ou lors d'un appel, ne jamais ouvrir une pièce jointe d'un courriel en cas de doute). La formation restreinte considère que ces informations, identifiées au jour de l'envoi du courriel d'information, auraient dû être transmises de manière synthétique aux personnes concernées.

196. D'autre part, la formation restreinte considère qu'en visant uniquement le risque d'emails, SMS ou appels frauduleux , la société n'a pas communiqué l'ensemble des principaux risques auxquels sont exposées les personnes concernées par la violation. La société les avait pourtant identifiés lors de sa notification initiale auprès de la CNIL, ainsi que dans les scripts de questions/réponses fournis aux conseillers répondant aux appels. A titre d'exemple, s'agissant du risque d'usurpation d'identité, dès lors que les personnes le découvrent généralement a posteriori, la formation restreinte estime qu'une mention de ce risque, susceptible de causer un préjudice important en cas de réalisation, associé à un renvoi vers la page dédiée du site cybermalveillance.gouv.fr, qui communique des informations sur les principaux signes dont il faut se méfier, aurait été plus efficace qu'un renvoi vers sa page d'accueil, compte tenu de la densité d'informations qui figurent sur ce site, et qui ne sont pas toutes appropriées au cas d'espèce. L'avantage d'une telle approche est de communiquer sur le risque et d'apporter des informations plus détaillées, sans nuire à l'ergonomie ni à la lisibilité de l'information.

197. En troisième lieu, la formation restreinte relève que la communication de la CNIL intitulée Violations massives de données en 2024 : quels sont les principaux enseignements et mesures à prendre du 28 janvier 2025 mentionnait des violations de données de différents responsables de traitement dont celle de la société. D'une part, elle estime que cette communication n'a pas accru le nombre de plaintes dès lors que dès décembre 2024, la CNIL avait déjà reçu la très grande majorité des plaintes sur les 2 614 reçues au jour de la notification du rapport le 25 juillet 2025, ce qui constituait un nombre record. D'autre part, la communication n'a pas augmenté le nombre de plaintes déposées à l'encontre des autres responsables de traitement cités.

198. Il résulte de ce qui précède que, le courriel d'information initial n'a pas constitué une communication appropriée, dès lors que les seules informations qu'il contenait ne permettaient pas aux millions de personnes concernées par la violation de données en cause d'être rassurées sur le fait que la société avait bien pris les mesures de remédiation nécessaires, ni de comprendre les risques auxquels elles étaient exposées, dont ceux liés à des emails, SMS ou appels frauduleux , ni les mesures à prendre pour s'en prémunir.

199. Dès lors, la formation restreinte considère que la société a commis un manquement à l'article 34 du RGPD en ne communiquant pas aux personnes concernées par la violation de données les informations nécessaires dès le premier

niveau d'information.

IV. Sur les mesures correctrices

200. Aux termes de l'article 20-IV de la loi n° 78-17 du 6 janvier 1978 modifiée, lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut […] saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes : […]

201. 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 les cas où le traitement est mis en œuvre par l'Etat, d'une astreinte dont le montant ne peut excéder 100 000 euros par jour de retard à compter de la date fixée par la formation restreinte ;

202. 7° À l'exception des cas où le traitement est mis en œuvre par l'État, une amende administrative ne pouvant excéder 10 millions d'euros ou, s'agissant d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Dans les hypothèses mentionnées aux 5 et 6 de l'article 83 du règlement (UE) 2016/679 du 27 avril 2016, ces plafonds sont portés, respectivement, à 20 millions d'euros et 4 % dudit chiffre d'affaires. La formation restreinte prend en compte, dans la détermination du montant de l'amende, les critères précisés au même article 83 .

203. L'article 83 du RGPD prévoit en outre que chaque autorité de contrôle veille à ce que les amendes administratives imposées en vertu du présent article pour des violations du présent règlement visées aux paragraphes 4, 5 et 6 soient, dans chaque cas, effectives, proportionnées et dissuasives , avant de préciser les éléments devant être pris en compte pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de cette amende.

204. Le deuxième alinéa de l'article 22 de la loi Informatique et Libertés dispose ensuite que la formation restreinte peut rendre publique les mesures qu'elle prend .

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

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

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

pour les violations visées aux paragraphes 4 à 6 de cet article 83, sur la notion d'" entreprise ", au sens de ces articles 101 et 102 TFUE (paragraphes 55 à 59).

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

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

209. A titre liminaire, la société reproche au rapporteur de retenir un manquement à la conservation des données, comme un grief autonome, et de considérer qu'il a aggravé le manquement à la sécurité, dès lors que l'attaquant a pu accéder à des données qui auraient dû être supprimées au jour de l'attaque. Elle considère également que le rapporteur propose de sanctionner deux fois les mêmes faits en prenant en compte le chiffre d'affaires de la maison mère des sociétés pour sanctionner à la fois la société FREE MOBILE et la société FREE, compte tenu de la violation des données des clients convergents. La société considère que le rapporteur méconnaît ainsi le principe non bis in idem .

210. Le rapporteur considère ne pas avoir méconnu le principe non bis in idem . Il précise que la violation de données en cause permet d'illustrer la gravité du manquement aux dispositions du RGPD relatives à la durée de conservation des données. Il propose à la formation restreinte de sanctionner les sociétés FREE MOBILE et FREE, deux personnes morales distinctes, pour des faits distincts, qui ont notamment impacté les données d'abonnés dits convergents .

211. La formation restreinte rappelle qu'il résulte de l'article 50 de la Charte des droits fondamentaux de l'Union européenne, relatif au principe non bis in idem que nul ne peut être poursuivi ou puni pénalement en raison d'une infraction pour laquelle il a déjà été acquitté ou condamné dans l'Union par un jugement pénal définitif conformément à la loi .

212. Elle rappelle également que ce principe a vocation à s'appliquer dans l'hypothèse où une personne a déjà été condamnée ou acquittée par un jugement définitif, pour des faits relevant de la même infraction (CJUE, 7 janvier 2004, Aalborg Portland e.a./Commission, affaire C 204/00 P, § 338).

213. En l'espèce, en premier lieu, la formation restreinte rappelle qu'elle considère que les faits relatifs à la conservation de l'intégralité des données de millions de contrats résiliés depuis plus de cinq ans, sans justification, au jour du contrôle, constituent un manquement à l'article 5-1-e du RGPD. Par ailleurs, les faits relatifs à l'insuffisance de mesures de sécurité permettant d'assurer la sécurité des données traitées constituent un manquement à l'article 32 du RGPD. Dès lors, la formation restreinte sanctionne la société au titre des articles 5-1-e) et 32 du RGPD pour des faits distincts, le manquement à l'article 5-1-e) n'étant pas un élément constitutif du manquement à l'article 32.

214. Par ailleurs, la formation restreinte rappelle qu'elle considère que les éléments du dossier portés à sa connaissance ne lui permettent pas de se prononcer sur le point de savoir si l'absence d'implémentation de la politique de durée de conservation des données a ou non permis à l'attaquant d'accéder à une profondeur historique de données plus importante, et donc de considérer que le manquement à l'article 5 du RGPD a aggravé le manquement à l'article 32 du RGPD.

215. En second lieu, la formation restreinte rappelle que la violation de données en cause, qui a notamment concerné les données de clients dits convergents, a été rendue possible ou a été facilitée par des vulnérabilités qui sont à la fois propres au système d'information de la société FREE MOBILE et propres à celui de la société FREE. Compte tenu de leurs responsabilités respectives à l'égard de leurs propres systèmes d'information, deux procédures de sanction distinctes ont été diligentées à l'encontre des deux sociétés. Dans le cadre de la procédure de sanction visant la société FREE MOBILE, la formation restreinte considère que celle-ci a commis un manquement à l'article 32 du RGPD, compte tenu des vulnérabilités propres à son système d'information (absence de sécurisation de la connexion au VPN, absence de moyens de détection des comportements suspects sur son VPN et son outil MOBO), qui ont été exploitées par l'attaquant lors de la violation de données en cause. Ces faits et leur imputation sont distincts de ceux imputés à la société FREE.

216. Dès lors, la formation restreinte considère ne pas méconnaitre le principe non bis in idem en sanctionnant deux personnes morales distinctes pour des faits distincts, ayant touché pour partie les mêmes données.

217. Par conséquent, la formation restreinte écarte le grief tiré d'une méconnaissance du principe non bis in idem .

1. Sur le prononcé d'une amende administrative

218. Le rapporteur propose à la formation restreinte de prononcer à l'encontre de la société une amende administrative au regard de manquements constitués aux articles 5-1-e), 32 et 34 du RGPD.

219. En défense, la société conteste l'analyse du rapporteur s'agissant des critères de l'article 83 du RGPD qui permettent de déterminer s'il y a lieu de prononcer une amende et de fixer son montant. Tout d'abord, s'agissant de la gravité de la violation de données, elle estime que, compte tenu de la recrudescence de la cybermenace, les données concernées

avaient donc déjà fait l'objet de violations antérieures. Elle fait notamment valoir qu'elle a pris toutes les mesures nécessaires pour remédier à la violation de données en cause, qui s'inscrit dans le cadre d'une recrudescence de cyberattaques, et pour atténuer les conséquences de celle-ci pour les personnes concernées. Par ailleurs, elle rappelle s'être mise en conformité en cours de procédure, avant la clôture de l'instruction, à l'égard des manquements relevés par le rapporteur. En outre, elle soutient ne pas avoir tiré d'avantages financiers de la violation de données et avoir, au contraire, subi un préjudice qui se traduit par la baisse du nombre des nouveaux abonnés au premier semestre de l'année 2025. Enfin, elle considère que la communication réalisée par la CNIL auprès des plaignants et sur son site web viole le secret de l'enquête et de l'instruction ainsi que sa présomption d'innocence, et doit être pris en compte.

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

221. En premier lieu, la formation restreinte considère qu'il y a lieu de faire application du critère prévu à l'alinéa a) relatif à la gravité du manquement compte tenu de la nature, de la portée ou de la finalité du traitement, ainsi que du nombre de personnes affectées et du niveau de dommage qu'elles ont subi.

222. La formation restreinte rappelle que les manquements commis ont concerné un nombre très important de personnes puisque, d'une part, la violation de données a concerné les données de plus de 24 millions de contrats d'abonnés et, d'autre part, la conservation injustifiée des données a concerné les données d'environ 15 millions de contrats. La formation restreinte observe que ce volume reflète la place centrale occupée par la société dans le secteur des télécommunications en France.

223. Par ailleurs, la formation restreinte a considéré que l'insuffisance des mesures de sécurité déployées par la société (l'authentification au VPN et la détection des comportements suspects) avait permis ou a facilité la survenance de la violation de données. Elle estime que le contexte de recrudescence de cyberattaques nécessite une attention particulière des responsables du traitement pour assurer la sécurité des données qu'ils traitent. En l'espèce, la violation de données a conduit à une surexposition des données et ainsi augmenté le risque d'utilisations frauduleuses.

224. En outre, la formation restreinte relève que sur les 24 633 469 contrats concernés par la violation de données, seules 58 239 personnes ont appelé le numéro de téléphone gratuit mis à disposition par les sociétés FREE et FREE MOBILE et ont donc bénéficié d'informations complètes sur les conséquences probables de la violation et les mesures que les personnes peuvent prendre pour les éviter. Ce défaut de communication d'informations essentielles à un très grand nombre de personnes a significativement augmenté la survenance des risques exposés au point 2 de la présente délibération.

225. Enfin, la formation restreinte observe que la violation de données en cause a généré un nombre sans précédent de plaintes adressées à la CNIL, ce qui reflète la grande inquiétude des personnes concernées. La formation restreinte relève que l'imprécision des courriels de notification adressés en application de l'article 34 du RGPD n'a pu qu'alimenter la crainte et l'incertitude des personnes s'agissant des conséquences de la violation sur leur vie privée.

226. Il résulte de ce qui précède que les manquements caractérisés à l'égard de la société sont particulièrement graves.

227. En deuxième lieu, la formation restreinte estime qu'il convient de tenir compte du critère prévu à l'article 83, paragraphe 2, b) du RGPD, relatif au fait que la violation ait été commise délibérément ou par négligence.

228. La formation restreinte considère que la société a fait preuve de négligence dès lors que le traitement a été mis en œuvre dès 2012 et qu'en 2024 (année du contrôle), elle n'avait pas mis en œuvre les mesures techniques lui permettant de s'assurer de conserver les données de ses anciens abonnés pendant une durée limitée. La formation restreinte précise que, compte tenu du fait que cette obligation préexistait à l'entrée en vigueur du RGPD, la société était tenue de purger les données dès la première échéance de conservation des données. A titre d'exemple, dès lors que la société soutient conserver les données à caractère personnel de ses anciens abonnés pendant cinq ans après la fin de la relation contractuelle à des fins de fraude, en cas de résiliation d'un abonné en 2012, la société aurait donc dû être en mesure de supprimer les données qui ne lui étaient plus nécessaires à des fins de fraude dès 2017.

229. S'agissant du manquement à l'article 32 du RGPD, la formation restreinte relève que les mesures de sécurité qui auraient permis d'empêcher ou de limiter la violation sont pourtant bien identifiées par l'état de l'art, et qu'elle disposait des moyens humains, techniques et financiers pour les mettre en œuvre.

230. Enfin, s'agissant du manquement à l'article 34 du RGPD, la société a fait preuve de négligence en ne portant pas à la connaissance des personnes concernées, dès le courriel de notification, les risques encourus par ces dernières, ainsi que les mesures qu'elles doivent prendre pour s'en prémunir alors même qu'elle les avait identifiés.

231. Par conséquent, la formation restreinte considère que les manquements en cause résultent de la négligence de la société.

232. En troisième lieu, la formation restreinte considère qu'il convient de faire application du critère prévu à l'alinéa k) de l'article 83, paragraphe 2 du RGPD relatif aux circonstances aggravantes ou atténuantes applicables aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation.

233. Outre le fait que le nombre d'abonnés a augmenté entre le dernier trimestre 2024 et le premier trimestre 2025, la formation restreinte relève que la société ne démontre pas le lien de causalité entre le préjudice subi du fait de la violation de données et une éventuelle perte de chiffre d'affaires qu'il conviendrait de prendre en compte en tant que circonstance atténuante.

234. Par ailleurs, s'agissant de la communication effectuée par la CNIL aux plaignants, la formation restreinte rappelle qu'elle s'inscrit dans le cadre de l'article 8-I-2-d) de la loi Informatique et Libertés modifiée, qui prévoit une obligation pour la Commission d'informer l'auteur d'une réclamation de l'issue de l'enquête (décision de sa Présidente de procéder à la clôture de la procédure de contrôle, et le cas échéant celle de la réclamation, ou d'engager une procédure de sanction). En l'espèce, la saisine de la formation restreinte et la désignation d'un rapporteur marquent la fin de la phase d'enquête au sens de l'article précité, et il convenait donc d'en informer l'auteur de la réclamation. La formation restreinte précise que le contenu de l'information communiquée aux plaignants ne comportait pas d'informations couvertes par le secret dès lors qu'il n'est pas fait mention des manquements reprochés ni de la mesure correctrice proposée par le rapporteur.

235. La formation restreinte rappelle également que, compte tenu de son impartialité et de son indépendance, elle n'est pas liée par les demandes formulées par le rapporteur dans le cadre d'une procédure de sanction. Dès lors, la décision de la présidente de la CNIL d'engager une procédure de sanction à l'encontre de la société ne préjuge pas de la décision qui sera rendue par les membres de la formation restreinte, ce que rappelait d'ailleurs le courrier d'information adressé par les services de la Commission aux plaignants.

236. En outre, s'agissant de la communication réalisée par la Commission sur son site web, la formation restreinte observe que, l'article intitulé Fuite de données et vol de votre IBAN : comment vous protéger si vous êtes concerné ? publié sur le site web de la CNIL le 8 août 2025 rappelle les risques encourus par les personnes concernées en cas d'usurpation de leur IBAN et formule des conseils pour s'en prémunir. La formation restreinte relève que cet article ne mentionne pas la société. La seule communication de la CNIL qui mentionne la société, comme victime d'une violation de données au même titre que d'autres acteurs également cités, s'intitule Violations massives de données en 2024 : quels sont les principaux enseignements et mesures à prendre ? et date du 28 janvier 2025. D'une part, la formation restreinte note que cet article ne comporte aucune information couverte par le secret de l'enquête (par exemple, le périmètre du contrôle, les manquements constatés), qui était en cours au moment de sa publication, ni aucun jugement de valeur sur la société. Cet article ne vise qu'à sensibiliser les organismes, dans un contexte de recrudescence de violations de données, aux modes opératoires utilisés par les attaquants, qui exploitent régulièrement les mêmes vulnérabilités. D'autre part, la formation restreinte observe qu'à la date de publication de cet article, la violation de données dont a été victime la société était déjà publique dès lors qu'elle avait été relayée sur le site web cybermalveillance.gouv.fr, ainsi que dans la presse.

237. Par conséquent, la formation restreinte estime que les communications de la CNIL ne sont pas de nature à constituer une circonstance atténuante.

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

2. Sur le montant de l'amende administrative

239. En défense, la société soutient que le montant de l'amende proposé par le rapporteur est disproportionné au regard des décisions antérieures de la formation restreinte. Elle ajoute qu'en prononçant une amende particulièrement élevée, la formation restreinte enverrait un mauvais signal aux autres responsables de traitement victimes d'une violation de données, qui pourraient décider ne pas porter à la connaissance de la Commission la survenance d'une violation de données et céder aux exigences des attaquants.

240. La formation restreinte relève d'abord que le manquement relatif à l'article 5-1-e) du RGPD est un manquement à l'un des principes clés du RGPD, susceptible de faire l'objet, en vertu de l'article 83 du RGPD, d'une amende administrative pouvant s'élever jusqu'à 20 000 000 euros et jusqu'à 4 % du chiffre d'affaires annuel, le montant le plus élevé étant retenu. Elle rappelle que les amendes administratives doivent être dissuasives et proportionnées.

241. Elle considère ensuite qu'il convient de recourir à la notion d' entreprise en droit de la concurrence, en vertu de la référence directe et explicite opérée à cette notion par le considérant 150 du RGPD ainsi que par les lignes directrices sur l'application et la fixation des amendes administratives aux fins du règlement 2016/679. Elle souligne en effet que dans des

arrêts rendus au titre du RGPD, la CJUE a confirmé que la notion d' entreprise contenue à l'article 83 du RGPD devait bien s'appréhender au regard du droit de la concurrence, régit par les articles 101 et 102 du TFUE (CJUE, grande chambre, 5 décembre 2023, C-807/21 et CJUE, cinquième chambre, 13 février 2025, C-383/23).

242. S'agissant de ce que recouvre la notion d' entreprise , la formation restreinte relève que dans son arrêt précité du 5 décembre 2023, la CJUE retient qu'une entreprise est une unité économique, même si du point de vue juridique cette unité économique est constituée de plusieurs personnes morales. La CJUE précise qu'à l'instar du droit de la concurrence (Cour de Cassation, ch. com., 7 juin 2023, pourvoi n° 22-10.545 ; Autorité de la concurrence, décisions n° 21-D-10 du 3 mai 2021 et n° 21-D-28 du 9 décembre 2021), lorsqu'une filiale est détenue directement ou indirectement à 100 % par sa maison mère, il existe une présomption réfragable selon laquelle la maison mère exerce une influence déterminante sur le comportement de la société. Pour déterminer le montant de l'amende envisagée, et qu'il corresponde à la capacité économique réelle de son destinataire, il convient alors, selon les deux arrêts précités, si les deux sociétés peuvent matériellement être regardées comme relevant de la même unité économique, de prendre en compte le chiffre d'affaires de la maison mère afin que l'amende soit effective, proportionnée et dissuasive.

243. En l'espèce, la formation restreinte rappelle que la société ILIAD détient à 100 % la société FREE MOBILE et considère ainsi, à l'instar du droit de la concurrence, qu'il existe une présomption selon laquelle la société ILIAD exerce une influence déterminante sur le comportement de la société FREE MOBILE sur le marché (CJUE, grande chambre, 5 décembre 2023, C-807/21 ; également CJUE, troisième chambre, 10 septembre 2009, Akzo C 97/08 P, paragraphes 58 à 61. Voir également, pour l'application de la présomption d'influence déterminante en cas de détention en chaîne : CJUE, Eni c/ Commission, 8 mai 2013 (C-508/11 P, § 48). Par conséquent, les sociétés ILIAD et FREE MOBILE constituent une seule entité économique et forment donc une seule entreprise au sens de l'article 101 du TFUE.

244. Compte tenu de ce qui précède, la formation restreinte considère qu'il y a lieu de retenir le chiffre d'affaires de l'entreprise au sens d' unité économique , à savoir celui de la maison mère du groupe. Elle rappelle qu'en 2024 le chiffre d'affaires de la société ILIAD était de 10,024 milliards d'euros pour un résultat net de 367 millions d'euros. La formation restreinte observe qu'au premier trimestre 2025, le chiffre d'affaires de la société ILIAD est de 2,5 milliards d'euros, dont 1,6 milliards provient de ses filiales françaises, dont la société FREE MOBILE. La formation restreinte relève également que le chiffre d'affaires de la société ILIAD, au premier trimestre 2025, est en hausse de 4,3 % par rapport au premier trimestre de l'année précédente.

245. S'agissant du montant de l'amende, la formation restreinte rappelle qu'il doit être proportionné et dissuasif, au regard des responsabilités et capacités financières de l'organisme mis en cause et des critères pertinents de l'article 83 du RGPD. Dès lors, le montant d'une amende est déterminé en fonction de chaque cas d'espèce. La formation restreinte relève notamment, en l'espèce, les ressources humaines, techniques et financières dont dispose la société pour respecter ses obligations au titre de la règlementation relative à la protection des données à caractère personnel, ainsi que le nombre particulièrement élevé de données et de personnes concernées par la violation de données (les données concernant 24 633 469 contrats) et les manquements en cause. Compte tenu de ce qui précède, la formation restreinte considère qu'apparait adapté de prononcer à l'encontre de la société FREE MOBILE une amende administrative d'un montant de 27 000 000 (vingt-sept millions) d'euros, au regard des manquements constitués aux articles 5-1-e), 32 et 34 du RGPD. Contrairement à ce que soutient la société, la formation restreinte considère que le prononcé de cette amende n'entraînera pas une absence de notification auprès de la Commission par d'autres responsables de traitement victimes d'une violation de données. La formation restreinte rappelle à cet égard que la notification d'une violation de données présentant un risque pour les droits et libertés des personnes à la CNIL constitue une obligation pour les responsables du traitement, dont la méconnaissance constitue un manquement à l'article 33 du RGPD pouvant donner lieu au prononcé d'une mesure correctrice par la formation restreinte.

B. Sur le prononcé d'une injonction

246. Dans son rapport initial, le rapporteur proposait à la formation restreinte de prononcer à l'encontre de la société une injonction de mettre en conformité le traitement avec les dispositions des articles 5-1-e) et 32 du RGPD, assortie d'une astreinte.

247. En défense, la société soutient que le prononcé d'une injonction est sans objet, dès lors qu'elle a déployé des mesures de mise en conformité en cours de procédure.

248. La formation restreinte relève qu'au jour de la séance, la société n'a pas justifié de l'évolution de l'ensemble des pratiques mises en cause dans le cadre de la procédure de sanction diligentée à son encontre. Dès lors, elle considère qu'afin de s'assurer de la mise en conformité de la société s'agissant des manquements relevés aux articles 5-1-e) et 32 du RGPD, le prononcé d'une injonction apparait nécessaire.

249. S'agissant du manquement à l'article 5-1-e) du RGPD, la formation restreinte considère que la société doit implémenter sa politique de durée de conservation des données, d'une part, en déployant un mécanisme de purge, au

sein de sa base de données, concernant les données des clients des contrats résiliés depuis plus de dix ans, d'autre part, en réalisant un tri afin de conserver, à des fins d'obligations comptables, pendant dix ans, uniquement les données qui lui sont strictement nécessaires.

250. […].

251. Par ailleurs, pour garantir le respect de cette injonction, la formation restreinte considère qu'au regard du chiffre d'affaires de la société et des moyens financiers, humains et techniques dont elle dispose pour remédier aux manquements constatés, il convient de prononcer une astreinte journalière d'un montant de 50 000 (cinquante mille) euros par jour de retard, liquidable à l'issue d'un délai de 6 (six) mois s'agissant de l'injonction relative à l'article 5-1-e) du RGPD et dans un délai de 3 (trois) mois s'agissant de l'injonction relative à l'article 32 du RGPD, à compter de la notification de la décision.

C. Sur la publicité de la sanction

252. La société conteste la proposition du rapporteur de rendre publique la présente délibération, compte tenu notamment de la sensibilité des mesures de sécurité visées dans le cadre de la procédure de sanction. Elle estime que la divulgation de ces mesures dans une décision publique pourrait porter atteinte à la sécurité de son système d'information.

253. La formation restreinte considère que la publicité de la présente décision se justifie au regard de la gravité des manquements, ainsi que du nombre de personnes concernées. Elle estime que la publicité permettra notamment d'informer l'ensemble des personnes concernées par les manquements en cause sur la nature de la mesure correctrice prise par la formation restreinte de la Commission à l'encontre de la société. Elle considère toutefois nécessaire que certains développements contenus dans la présente délibération seront occultés.

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

PAR CES MOTIFS

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

- prononcer à l'encontre de la société FREE MOBILE, une amende administrative d'un montant de 27 000 000 (vingt-sept millions) d'euros au regard des manquements constitués aux articles 5-1-e), 32 et 34 du RGPD ;

- prononcer une injonction, à l'encontre de la société FREE MOBILE de mettre en conformité le traitement avec les dispositions des articles 5-1-e) et 32 du RGPD, et en particulier :

o S'agissant du manquement à l'article 5-1-e) du RGPD, d'implémenter sa politique de durée de conservation des données, dans un délai de six mois, en effectuant :

• une purge au sein de la base de données de la société s'agissant des données des clients des contrats résiliés depuis plus de 10 ans ;

• un tri parmi les données afin de conserver pendant 10 ans uniquement les données strictement nécessaires à des fins comptables ;

o S'agissant du manquement à l'article 32 du RGPD, de mettre en œuvre les mesures techniques et organisationnelles appropriées, dans un délai de trois mois, afin de garantir un niveau de sécurité adapté au risque, notamment :

• […];

• […];

• […];

- assortir l'injonction d'une astreinte de 50 000 (cinquante mille) euros par jour de retard, les justificatifs de la mise en conformité devant être adressés à la formation restreinte dans les délais précités ;

- de rendre publique, sur le site de la CNIL et sur le site de Légifrance, sa délibération, qui n'identifiera plus nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.

Le Président

Philippe-Pierre CABOURDIN

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