Délibération SAN-2023-023 du 29 décembre 2023

Commission Nationale de l'Informatique et des Libertés

Nature de la délibération : Sanction
Date de publication sur Légifrance : Jeudi 11 janvier 2024
Etat juridique : En vigueur

Délibération de la formation restreinte n°SAN-2023-023 du 29 décembre 2023 concernant la société NS CARDS FRANCE

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de M. Alexandre LINDEN, président, M. Philippe-Pierre CABOURDIN, vice-président, M. Alain DRU et Mme Isabelle LATOURNARIE-WILLEMS, membres ;

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

Vu la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ;

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

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

Vu la délibération no 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision n° 2021-193C du 29 juin 2021 de la présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification des traitements de données à caractère personnel mis en œuvre par la société ou pour son compte ;

Vu la décision de la présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur devant la formation restreinte, en date du 29 mars 2022 ;

Vu le rapport de M. François PELLEGRINI, commissaire rapporteur, notifié à la société NS CARDS FRANCE le 3 juillet 2023 ;

Vu les observations écrites versées par la société NS CARDS FRANCE le 18 août 2023 ;

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte du 16 novembre 2023 :

- M. François PELLEGRINI, commissaire, entendu en son rapport ;

En qualité de représentants de la société NS CARDS FRANCE :

- […];

- […];

- […];

La société NS CARDS FRANCE ayant eu la parole en dernier ;

La formation restreinte a adopté la décision suivante :

I. Faits et procédure

1. La société NS CARDS FRANCE (ci-après " la société "), dont le siège social est situé 10, rue Vandrezanne à Paris (75013), a été immatriculée au registre du commerce et des sociétés le 9 novembre 2010. En 2019, son chiffre d'affaires s'élevait à […] euros pour un résultat net de […] euros et en 2020, son chiffre d'affaires s'élevait à […] euros pour un résultat net de […] euros. En 2023, elle comptait six salariés.

2. La société NS CARDS FRANCE est un distributeur de monnaie électronique qui permet d'effectuer des paiements en ligne. La société propose deux formes de solutions de paiement : d'une part, elle distribue, dans des points de vente agréés, des coupons neosurf au moyen desquels des particuliers peuvent effectuer des paiements en ligne sur des sites web partenaires ; d'autre part, l'utilisation de coupons neosurf peut également être adossée à la création d'un porte-monnaie électronique, laquelle nécessite de créer un compte utilisateur sur le site web www.neosurf.com ou l'application mobile " neosurf " et de le créditer au moyen des coupons ou d'une carte bancaire. La création d'un compte utilisateur permet d'effectuer des paiements en ligne ou de recevoir des gains. C'est cette seconde activité qui est en cause dans la présente procédure.

3. Deux missions de contrôle ont eu lieu en application de la décision n° 2021-193C du 29 juin 2021 de la présidente de la CNIL afin de vérifier le respect par la société de l'ensemble des dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après " le RGPD ") et de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée (ci-après " la loi Informatique et Libertés "). Le 24 septembre 2021, les services de la CNIL ont effectué un contrôle en ligne à partir du site web " www.new.neosurf.com ". Le 13 octobre 2021, les services de la CNIL ont procédé à un contrôle sur place dans les locaux de la société NS CARDS FRANCE, situés à Paris (75013).

4. Le contrôle en ligne du site web www.new.neosurf.com (devenu www.neosurf.com) avait principalement pour objet de vérifier les modalités d'information des personnes et la procédure de création d'un compte utilisateur. Il a permis de constater le dépôt de cookies et autres traceurs via ledit site web. Le contrôle sur place a plus spécifiquement porté sur la vérification de la documentation exigée par le RGPD, le processus de création de compte sur l'application mobile neosurf, les durées de conservation appliquées aux données des comptes utilisateurs ainsi que sur les mesures techniques et organisationnelles destinées à assurer la sécurité des données collectées au moyen du site web et de l'application mobile.

5. Ces deux missions de contrôle ont donné lieu à l'établissement des procès-verbaux n° 2021-193/1 et 2021-193/2. Par courriers des 8 octobre, 22 octobre et 15 novembre 2021, la société a transmis aux services de la Commission des éléments complémentaires.

6. Conformément à l'article 56 du RGPD, la CNIL a informé le 10 mai 2023 l'ensemble des autorités de contrôle européennes de sa compétence pour agir en tant qu'autorité de contrôle cheffe de file concernant les traitements transfrontaliers mis en œuvre par la société, résultant de ce que l'établissement unique de la société se trouve en France. Après échange entre la CNIL et les autorités de protection des données européennes dans le cadre du mécanisme de guichet unique, il apparaît que les autorités allemande, autrichienne, belge, chypriote, danoise, espagnole, finlandaise, grecque, irlandaise, italienne, luxembourgeoise, néerlandaise, norvégienne, polonaise, portugaise, roumaine et suédoise sont concernées par le traitement, des comptes utilisateurs ayant été créés par des résidents de ces États.

7. Aux fins d'instruction de ces éléments, la présidente de la Commission a, le 29 mars 2022, désigné M. François PELLEGRINI en qualité de rapporteur sur le fondement de l'article 22 de la loi Informatique et Libertés.

8. Le 3 juillet 2023, le rapporteur a fait notifier à la société un rapport détaillant les manquements aux articles 5-1-e), 12, 13 et 32 du RGPD ainsi qu'à l'article 82 de la loi Informatique et Libertés, qu'il estimait constitués en l'espèce.

9. Le 18 août 2023, la société a produit ses observations en réponse au rapport de sanction.

10. Par courrier du 29 septembre 2023, le rapporteur a informé le conseil de la société que l'instruction était close, en application de l'article 40, III, du décret modifié n° 2019-536 du 29 mai 2019.

11. Par courrier du 2 octobre 2023, la société a été informée que le dossier était inscrit à l'ordre du jour de la formation restreinte du 16 novembre 2023.

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

II. Motifs de la décision

A. Sur la procédure de coopération européenne

13. En application de l'article 60 paragraphe 3 du RGPD, le projet de décision adopté par la formation restreinte a été transmis le 29 novembre 2023 aux autorités de contrôle européennes concernées.

14. Au 28 décembre 2023, aucune des autorités de contrôle concernées n'avait formulé d'objection pertinente et motivée à l'égard de ce projet de décision, de sorte que, en application de l'article 60, paragraphe 6, du RGPD, ces dernières sont réputées l'avoir approuvé.

B. Sur le manquement à l'obligation de limitation de la durée de conservation des données

15. Aux termes de l'article 5-1, 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 ".

16. Le rapporteur a relevé que lors de la création d'un compte utilisateur sur le site web www.neosurf.com, le nom, le prénom, la date de naissance, l'adresse postale, l'adresse courriel, le numéro de téléphone et, le cas échéant, les coordonnées bancaires étaient collectés, de même que des documents personnels, tels que des justificatifs d'identité et de domicile. Or, le rapporteur a relevé qu'il ressortait du contrôle sur place que si la société avait défini une durée de conservation de dix ans de ces données à compter de la dernière opération effectuée sur le compte, dans les faits, les comptes étaient uniquement inactivés à l'issue de cette durée, tandis que ces données étaient conservées en base de production pour une durée indéterminée. Il a également relevé qu'aucune purge n'avait été réalisée dans les bases de données de la société depuis le début de son activité en 2005. Le rapporteur a notamment estimé que le courrier de la société du 15 novembre 2021 montrait la conservation de 70 049 comptes inactifs depuis plus de dix ans. En outre, il a estimé que la société ne justifiait pas de l'application de la nouvelle durée de conservation de cinq ans qu'elle a définie à la suite des contrôles de la CNIL pour les données de comptes utilisateurs. Enfin, il a relevé que 51 735 comptes étaient conservés sans finalité, dans la mesure où ceux-ci étaient " non confirmés ", c'est-à-dire que l'adresse électronique n'avait pas été confirmée lors de la création du compte.

17. En défense, lors de l'instruction, la société a tout d'abord indiqué avoir défini une durée de conservation des comptes utilisateurs de dix ans à des fins de lutte contre le blanchiment et le financement du terrorisme (" LCB-FT ") avant de déclarer, dans son courrier du 15 novembre 2021, que cette durée n'était désormais plus appliquée qu'aux contrats clients conclus pour un montant supérieur à 120 € HT, en application de l'article D. 213-1 du code de la consommation, et que les autres données de comptes utilisateurs seraient désormais conservées cinq ans à compter de la dernière opération effectuée sur le compte. Dans ses observations en réponse, la société a en outre rectifié les déclarations effectuées lors de l'instruction quant à la durée applicable à la conservation de certaines données à des fins de LCB-FT, qui est de cinq ans en application de l'article 561-2 du code monétaire et financier. La société soutient que la requête fournie concernant les 70 049 comptes inactifs montrerait la présence de ces comptes en base depuis dix ans et non depuis plus de dix ans. Elle précise que cette requête avait seulement pour objectif de montrer l'application effective de la nouvelle durée de conservation de cinq ans qu'elle avait définie. Dans ses observations, la société fournit une nouvelle capture d'écran qui attesterait sans ambiguïté de la suppression des comptes inactifs depuis cinq ans.

18. S'agissant des 51 735 comptes non confirmés, la société affirme que les données associées à ces comptes sont conservées un an, puis supprimées à défaut de confirmation du compte. Elle déclare que la finalité poursuivie par cette conservation est de permettre aux utilisateurs de disposer d'un temps adéquat pour confirmer leur compte et reproche au rapporteur d'avoir préjugé d'une conservation excessive des données associées aux comptes non confirmés, sans même l'interroger sur la finalité du traitement et la durée de conservation appliquée à ces données.

19. La formation restreinte rappelle, d'une part, que la durée de conservation des données à caractère personnel doit être déterminée en fonction de la finalité poursuivie par le traitement. Lorsqu'elles ne sont plus nécessaires au besoin de la finalité pour laquelle elles ont été collectées, les données doivent soit être supprimées, soit faire l'objet d'un archivage intermédiaire lorsque leur conservation est nécessaire pour le respect d'obligations légales ou à des fins précontentieuses ou contentieuses. Les données ainsi placées en archivage intermédiaire le sont pour une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont conservées, conformément aux dispositions en vigueur. Ainsi, après avoir opéré un tri des données pertinentes à archiver, le responsable de traitement doit prévoir, à cet effet, une base de données d'archives dédiée ou une séparation logique dans la base de données active. Cette séparation logique est assurée par la mise en place de mesures techniques et organisationnelles garantissant que seules les personnes ayant un intérêt à traiter les données en raison de leurs fonctions puissent y accéder. Au-delà de ces durées de conservation en archive intermédiaire, les données à caractère personnel doivent, sauf exception, être supprimées ou anonymisées (CNIL, FR, 8 septembre 2022, Sanction, Groupement X, n° SAN-2022-018, publié).

20. D'autre part, aux termes de l'article L. 213-1 du code de la consommation : "

Lorsque le contrat est conclu par voie électronique et qu'il porte sur une somme égale ou supérieure à un montant fixé par décret, le contractant professionnel assure la conservation de l'écrit qui le constate pendant un délai déterminé par ce même décret et en garantit à tout moment l'accès à son cocontractant si celui-ci en fait la demande. ". L'article D. 213-1 du même code prévoit que " [l]e montant mentionné à l'article L. 213-1 est fixé à 120 euros " et l'article D. 213-2 dispose que " [l]e délai mentionné à l'article L. 213-1 est fixé à dix ans à compter de la conclusion du contrat lorsque la livraison du bien ou l'exécution de la prestation est immédiate. Dans le cas contraire, le délai court à compter de la conclusion du contrat jusqu'à la date de livraison du bien ou de l'exécution de la prestation et pendant une durée de dix ans à compter de celle-ci ".

21. En l'espèce, la formation restreinte relève tout d'abord, s'agissant de la conservation de 51 735 comptes non confirmés en base, que si le courrier de la société du 15 novembre 2021 indiquait que les données des " prospects inactifs " étaient supprimées après un an, la politique de durées de conservation jointe à ce courrier prévoyait paradoxalement une durée de conservation de trois ans des données liées à la " gestion des fichiers prospects non clients ". Lors de l'audience, la société a expliqué cette contradiction par la circonstance que la durée de conservation de trois ans visait uniquement la conservation à des fins de prospection commerciale et qu'elle ne se livrait plus à ce type d'activité. En tout état de cause, la formation restreinte considère que dans ses observations en défense, la société justifie d'une durée et d'une finalité pour la conservation des données de comptes non confirmés, à savoir, une conservation d'un an afin de permettre aux personnes concernées de disposer d'un temps adéquat pour confirmer leur compte. Partant, elle considère que les éléments du dossier ne permettent pas de caractériser un manquement à l'article 5-1-e) du RGPD sur ce point.

22. Ensuite, la formation restreinte relève qu'à la date du contrôle sur place, la société a défini une durée de dix ans, qui commence à courir à la date de l'activation du compte utilisateur. Néanmoins, elle relève qu'à l'issue de cette durée, les comptes utilisateurs étaient inactivés mais que la société continuait à conserver les données des comptes en base de données pour une durée indéterminée. La formation restreinte relève en outre que selon les déclarations de la société elle-même, aucune purge des données n'avait été effectuée depuis 2005.

23. S'agissant de la conservation de 70 049 comptes inactifs, la formation restreinte relève que la capture d'écran fournie par la société dans son courrier du 15 novembre 2021 était destinée à illustrer, à la demande des services de la CNIL, " le nombre de comptes inactifs ayant une date de création supérieure à 10 ans à compter du 13 octobre 2021 ". La formation restreinte considère qu'au vu des explications fournies par la société, la capture d'écran produite montrait la conservation de comptes inactifs depuis dix ans et non depuis plus de dix ans.

24. Néanmoins, la formation restreinte relève qu'il résulte de ce qui précède que lorsque la durée de conservation est atteinte, les données personnelles doivent être supprimées ou anonymisées et que le fait de rendre un compte inactif ne correspond ni à une suppression des données personnelles qu'il contient, ni à une anonymisation. Dès lors, il ressort des pièces du dossier qu'à la date du contrôle sur place, la société conservait les données de comptes utilisateurs, même inactivés, pour une durée indéterminée.

25. En tout état de cause, la formation restreinte observe qu'il ressort de la capture d'écran susmentionnée comme des autres éléments du dossier que jusqu'aux contrôles effectués par les agents de la CNIL, les données de 70 049 comptes clients étaient présentes en base depuis dix ans sans qu'aucun tri n'ait été effectué entre les données à conserver conformément aux dispositions de l'article D. 213-1 du code de la consommation et celles à supprimer. La formation restreinte note que la durée de conservation de cinq ans des données autres que celles visées par cette disposition n'a été définie qu'à l'issue du contrôle sur place, comme l'a confirmé la société dans son courrier du 15 novembre 2021 et que la preuve de son application effective n'a été apportée que dans le cadre de ses observations en défense, le 18 août 2023. Partant, la formation restreinte considère que la société a conservé les données de comptes non concernées par l'article D. 213-1 du code de la consommation pour des durées excessives.

26. En conséquence, la formation restreinte considère que les faits qui précèdent caractérisent un manquement à l'article 5-1-e) du RGPD. La formation restreinte relève que la société s'est mise en conformité au cours de la procédure avec la mise en place et l'application de durées de conservation adéquates des données de comptes utilisateurs, au regard des différentes finalités poursuivies. Elle rappelle néanmoins que cette mise en conformité ne saurait exonérer la société de sa responsabilité pour le passé.

C. Sur le manquement à l'obligation d'information des personnes

27. En vertu de l'article 12 du Règlement, le responsable de traitement doit fournir aux personnes concernées les informations prévues à l'article 13 du même Règlement " d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples […] ".

28. L'article 13 du RGPD dresse quant à lui la liste des informations devant être fournies à la personne concernée lorsque les données à caractère personnel sont collectées directement auprès d'elle. Ces informations portent notamment sur l'identité du responsable de traitement et ses coordonnées, les finalités du traitement mis en œuvre, sa base juridique, les

destinataires ou les catégories de destinataires des données, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données vers un pays tiers. L'article impose également au responsable de traitement, lorsque cela apparaît nécessaire pour garantir " un traitement équitable et transparent " des données personnelles en l'espèce, d'informer les personnes sur la durée de conservation des données, l'existence des différents droits dont bénéficient les personnes, l'existence du droit de retirer son consentement à tout moment et le droit d'introduire une réclamation auprès d'une autorité de contrôle.

29. Le Règlement ne prescrit pas la forme au moyen de laquelle ces informations doivent être fournies. En pratique, ces informations sont généralement regroupées au sein d'une politique de confidentialité.

30. Dans son rapport, le rapporteur relève en substance que l'information fournie par la société sur le site web www.neosurf.com et sur son application mobile via la politique de confidentialité était incomplète, non à jour et uniquement en anglais. Le rapporteur note toutefois que la société s'est, depuis les contrôles, engagée dans une démarche de mise en conformité, sans que cela remette en cause les manquements pour le passé.

31. En défense, la société ne conteste pas le manquement, mais indique s'être mise en conformité depuis les contrôles. Elle reproche au rapporteur de fonder certains griefs de son rapport sur des vérifications informelles au terme desquelles il aurait constaté que des carences perduraient au jour de l'envoi du rapport, en dehors de toute constatation actée contradictoirement dans un procès-verbal.

32. La formation restreinte relève tout d'abord qu'il ressort des constats réalisés lors des contrôles que s'agissant du site web www.neosurf.com, une politique de confidentialité disponible en pied de page d'accueil du site était disponible uniquement en anglais. A cet égard, elle relève, à l'instar du rapporteur, que l'information fournie au moyen d'une politique de confidentialité disponible uniquement en anglais, relative à des traitements de données ciblant majoritairement un public francophone, ne permet pas aux personnes concernées d'apprécier à l'avance la portée et les conséquences des traitements et n'est par conséquent pas conforme aux exigences de transparence de l'information posées par l'article 12 du RGPD. La formation restreinte considère qu'il en va de même du renvoi opéré vers la politique de confidentialité uniquement en anglais depuis le formulaire de création de compte.

33. Ensuite, la formation restreinte relève que la page d'accueil du site web et la page de création de compte utilisateur renvoyaient toutes deux vers des versions de la politique de confidentialité de 2018 et de 2021, lesquelles ne mentionnaient ni la durée de conservation des données ni le droit d'introduire une réclamation auprès de la CNIL. La formation restreinte note qu'eu égard aux données traitées par la société, incluant des coordonnées bancaires, ces informations étaient nécessaires pour garantir un traitement équitable et transparent au sens de l'article 13(2) du RGPD. Elle relève en outre, à l'instar du rapporteur, que la coexistence de ces deux versions incomplètes de la politique de confidentialité était susceptible de créer une confusion chez les personnes concernées quant à l'étendue des droits dont elles disposaient à l'égard de leurs données et aux conséquences du traitement de ces dernières.

34. S'agissant de l'application mobile neosurf, la formation restreinte relève qu'à la date des contrôles, la page de création de compte proposait également une politique de confidentialité incomplète datée de 2018, disponible uniquement en anglais, méconnaissant de la même manière les articles 12 et 13 du RGPD pour les raisons déjà développées s'agissant du site web.

35. En conséquence, la formation restreinte considère que la société a commis un manquement aux articles 12 et 13 du RGPD. Elle précise que le manquement pris en compte est celui qui a été cristallisé au moment des contrôles et que les vérifications informelles du rapporteur ayant précédé la notification de son rapport avaient uniquement vocation à attirer l'attention de la société sur le fait que sa conformité n'était pas encore atteinte. La formation restreinte prend acte de ce que la société s'est mise en conformité.

D. Sur les manquements à l'obligation d'assurer la sécurité des données

36. Aux termes de l'article 32 du RGPD, *" 1. 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 ".

1. Sur les mots de passe des comptes utilisateurs

37. Pour proposer à la formation restreinte de considérer que la société avait méconnu ses obligations résultant de l'article 32 du RGPD, le rapporteur a relevé que lors du contrôle en ligne, la délégation avait tout d'abord constaté que lors de la création d'un compte utilisateur sur le site web de la société, les mots de passe de six caractères composés de trois catégories de caractères (majuscules, minuscules et chiffres) étaient acceptés et qu'aucune restriction d'accès en cas d'échec d'authentification n'était mise en œuvre. En outre, il a relevé que 49 214 mots de passe étaient inscrits en clair au sein de la base de données de la société et associés à leur adresse électronique ainsi qu'à leur identifiant. Enfin, le rapporteur a relevé que les mots de passe qui n'étaient pas conservés en clair étaient stockés sous une forme hachée et salée au moyen de la fonction SHA-1, réputée obsolète.

38. En défense, la société ne conteste pas les manquements, mais déclare avoir pris des actions correctives. Tout d'abord, elle annonce avoir adapté sa politique de mots de passe afin d'atteindre le taux d'entropie minimal de 50 bits recommandé par la CNIL lorsque ce mot de passe est accompagné d'une mesure de restriction d'accès et indique que la mise en place de ces nouvelles mesures a été finalisée en août 2023. Elle reproche en outre au rapporteur de s'appuyer sur des vérifications informelles qui lui auraient permis de constater une entropie toujours insuffisante à la date de l'envoi du rapport. Ensuite, la société précise que l'accès à des mots de passe en clair était dû à des contraintes techniques liées à la mise en œuvre de mesures de chiffrement des mots de passe d'anciens comptes créés au début de son activité et qu'au jour de ses observations en défense, tous les mots de passe sont chiffrés au sein de la base de données. Enfin, la société prend acte des conclusions du rapporteur concernant l'utilisation de l'algorithme de hachage SHA-1 et annonce avoir opté pour un basculement vers la norme SHA-512, effectif depuis le mois de juillet 2023.

39. En premier lieu, la formation restreinte rappelle qu'il résulte des dispositions de l'article 32 du RGPD que le responsable de traitement est tenu de s'assurer que le traitement automatisé de données qu'il met en œuvre est suffisamment sécurisé. Le caractère suffisant des mesures de sécurité s'apprécie, d'une part, au regard des caractéristiques du traitement et des risques qu'il induit, d'autre part, en tenant compte de l'état de connaissances et du coût des mesures.

40. La formation restreinte considère tout d'abord que des règles de complexité des mots de passe trop permissives, qui autorisent l'utilisation de mots de passe insuffisamment robustes, peuvent conduire à des attaques par des tiers non autorisés, telles que des attaques par " force brute " ou " par dictionnaire ", qui consistent à tester successivement et de façon systématique de nombreux mots de passe et conduisent, ainsi, à une compromission des comptes associés et des données à caractère personnel qu'ils contiennent.

41. Elle relève, à cet égard, que la nécessité d'un mot de passe fort est recommandée tant par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) que par la Commission dans sa délibération n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe, exigence confirmée dans sa délibération n° 2022-100 du 21 juillet 2022.

42. A titre d'illustration, le rapporteur rappelle que la Commission considère dans sa délibération n° 2017-012 du 19 janvier 2017 – qui n'a certes pas un caractère impératif mais qui fournit un éclairage pertinent sur les mesures qu'il convient de prendre en matière de sécurité – que, pour assurer un niveau de sécurité et de confidentialité suffisant, dans l'hypothèse où l'authentification repose uniquement sur un identifiant et un mot de passe, ce dernier doit être composé d'au minimum douze caractères comprenant des majuscules, des minuscules, des chiffres et des caractères spéciaux.

43. À défaut, la Commission considère que permet également d'assurer un niveau de sécurité et de confidentialité suffisant une authentification reposant sur un mot de passe d'une longueur minimum de huit caractères, composé de trois catégories de caractères différentes mais accompagnée d'une mesure complémentaire comme, par exemple, la temporisation d'accès au compte après plusieurs échecs (suspension temporaire de l'accès dont la durée augmente à mesure des tentatives), la mise en place d'un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (ex : " captcha ") et/ou le blocage du compte après plusieurs tentatives d'authentification infructueuses (au maximum dix).

44. La formation restreinte souligne qu'elle a, à plusieurs reprises, adopté des sanctions pécuniaires où la caractérisation d'un manquement à l'article 32 du RGPD est le résultat de mesures insuffisantes pour garantir la sécurité des données traitées. Les délibérations n° SAN-2019-006 du 13 juin 2019, n° SAN-2019-007 du 18 juillet 2019 et n° SAN-2022-018 du 8 septembre 2022 visent notamment l'insuffisante robustesse des mots de passe.

45. Ensuite, la formation restreinte rappelle que 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 qu'ils 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/).

46. 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 ". 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.

47. La formation restreinte relève qu'en l'espèce, les mots de passe des utilisateurs du site web www.neosurf.com devaient être, à l'époque des contrôles, composés de six caractères de trois sortes et dépourvus de mesure de sécurité complémentaire.

48. Elle considère qu'une telle construction ne permettait pas d'assurer la sécurité des données et d'empêcher que des tiers non autorisés y aient accès. La formation restreinte rappelle que, comme l'a souligné le rapporteur, la société traitait au jour du contrôle sur place les données de près de 700 000 comptes utilisateurs, telles que les nom, prénom, date de naissance et adresse courriel, adresse postale, numéro de téléphone, mais également des coordonnées bancaires (lorsque l'utilisateur décide d'y adosser un porte-monnaie électronique) ou encore des justificatifs d'identité et de domicile (lorsqu'un règlement excède un certain montant). Or, une authentification reposant sur l'utilisation d'un tel mot de passe, court et dépourvu de mesure de sécurité complémentaire, peut conduire à des attaques par des tiers non autorisés et ainsi à une compromission des comptes utilisateurs et des nombreuses données à caractère personnel qu'ils contiennent.

49. En conséquence, la formation restreinte considère que la politique de mots de passe déployée n'était pas suffisamment robuste pour garantir la sécurité des données traitées, ce qui méconnaît l'article 32 du RGPD.

50. En deuxième lieu, la formation restreinte relève que la conservation en clair des mots de passe d'utilisateurs, associés à leurs identifiants et à leur adresse courriel, ne permet pas de garantir leur sécurité. Cette modalité de conservation implique que toute personne ayant accès à la base de données des clients de la société peut les consulter et les collecter. Ces mots de passe des utilisateurs, associés à leurs identifiants, permettent d'accéder à toutes les données à caractère personnel contenues dans leurs comptes neosurf, voire à d'autres comptes de services, les mêmes identifiants et mots de passe étant, comme l'a souligné le rapporteur, souvent utilisés pour accéder à plusieurs services.

51. Dans ces conditions, la formation restreinte considère que les modalités de stockage des mots de passe ne permettaient pas, au jour des constats, de garantir la sécurité et la confidentialité des données à caractère personnel des détenteurs de comptes néosurf, ce qui méconnaît l'article 32 du RGPD.

52. En troisième lieu, la formation restreinte rappelle que le recours à la fonction SHA-1 pour le hachage des mots de passe n'est plus considéré comme conforme à l'état de l'art, ainsi qu'il ressort en particulier du guide de sélection d'algorithmes cryptographiques édité par l'ANSSI, en date du 8 mars 2021, qui indique que celle-ci est " proscrite pour une utilisation générale ". La formation restreinte relève en outre qu'en l'état actuel de la technique, la CNIL a établi des recommandations spécifiques dans son guide au profit des développeurs, en recommandant de stocker les mots de passe " sous forme de hachage (hash) au moyen d'une librairie éprouvée, comme Argon2, yescrypt, scrypt, balloon, bcrypt et, dans une moindre mesure, PBKDF2 "(https://lincnil.github.io/Guide-RGPD-du-developpeur/).

53. En conséquence, la formation restreinte considère que les faits précités, non contestés par la société, constituent des manquements aux obligations de l'article 32 du RGPD. Elle prend acte de ce que depuis les contrôles, la société a remédié aux manquements constatés en mettant en place une politique de mots de passe présentant un niveau de sécurité adéquat, en chiffrant l'ensemble des mots de passe et en justifiant de la mise en œuvre d'un système de hachage satisfaisant desdits mots de passe, en SHA-512.

2. Sur le partage de l'accès à la base de données clients

54. Le rapporteur relève que, lors du contrôle sur place, la délégation a été informée que le compte utilisé pour l'accès à la base de données clients était partagé par l'équipe de développement.

55. En défense, la société conteste l'existence du manquement. Elle fait valoir que seul un salarié dispose d'un accès restreint à la base de données pour réaliser ses missions en tant que développeur, et qu'une seconde personne est habilitée à accéder à cette base dans le cadre de sa mission d'administrateur de base de données. Elle précise que la procédure de connexion s'effectue par bastion, c'est-à-dire via un serveur de connexion intermédiaire qui permet ensuite d'accéder à la base, et que seul l'accès au bastion est partagé. Une fois connecté au bastion, la connexion à la base de données serait permise par un identifiant et un mot de passe complexe de seize caractères : la société indique que l'administrateur de la base et le développeur disposent d'identifiants et de mots de passe distincts pour se connecter à la

base de données et que la connexion est filtrée par adresse IP, ce qui permettrait de préserver la traçabilité des accès à la base.

56. La formation restreinte relève qu'il ressort des explications fournies par la société que l'équipe de développement est composée d'un seul salarié et que, dès lors, seules deux personnes sont habilitées à accéder à la base de données clients à savoir, d'une part, l'administrateur de la base et, d'autre part, le développeur qui dispose d'un accès restreint à cette base. La formation restreinte note également que le développeur, comme l'administrateur, disposent d'un compte d'accès individuel à cette base.

57. En conséquence, la formation restreinte considère que le manquement n'est pas constitué.

E. Sur le manquement aux obligations de l'article 82 de la loi Informatique et Libertés

58. L'article 82 de la loi Informatique et Libertés dispose que : *" tout abonné ou utilisateur d'un service de communications électroniques doit être informé de manière claire et complète, sauf s'il l'a été au préalable, par le responsable du traitement ou son représentant :*

1° De la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement ;

2° Des moyens dont il dispose pour s'y opposer.

Ces accès ou inscriptions ne peuvent avoir lieu qu'à condition que l'abonné ou la personne utilisatrice ait exprimé, après avoir reçu cette information, son consentement qui peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle.

Ces dispositions ne sont pas applicables si l'accès aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur :

1° Soit, a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ;

2° Soit, est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur ".

59. Ces dispositions transposent en droit français l'article 5, paragraphe 3, de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (dite " directive e-Privacy ").

1. Sur le dépôt de cookies Google Analytics sur le terminal de l'utilisateur sans recueil de son consentement

60. Le rapporteur relève que lors du contrôle en ligne, la délégation a constaté le dépôt de treize cookies avant toute action de l'utilisateur dès son arrivée sur la page d'accueil du site web www.neosurf.com, au nombre desquels figurent des cookies de mesure d'audience de Google Analytics, qui auraient dû être soumis au consentement préalable de l'utilisateur.

61. En défense, la société a d'abord soutenu lors de l'instruction que le cookie Google Analytics était un outil de mesure d'audience à usage interne exempté du recueil du consentement, avant de reconnaître les faits dans ses observations en défense et d'annoncer ne plus utiliser cet outil. Elle communique une pièce attestant de ce qu'à la date du 16 août 2023, les cookies Google Analytics ne sont plus déposés sur le terminal des utilisateurs du site et de l'application neosurf.

62. La formation restreinte rappelle que l'article 82 de loi Informatique et Libertés prévoit que les opérations d'accès ou d'inscription d'informations dans le terminal d'un utilisateur ne peuvent avoir lieu qu'après que ce dernier a exprimé son consentement, seuls les cookies ayant pour finalité exclusive de permettre ou de faciliter la communication par voie électronique ou ceux strictement nécessaires à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur étant exemptés de cette obligation.

63. La formation restreinte considère qu'il ressort de la documentation mise en ligne par la société GOOGLE que, d'une part, en fonction du paramétrage retenu par l'éditeur du site concerné, les cookies Google Analytics peuvent comporter des fonctionnalités publicitaires et que, d'autre part, quel que soit le paramétrage retenu concernant les fonctionnalités publicitaires précitées, les données collectées via les cookies Google Analytics peuvent être réutilisées pour maintenir et protéger le service Analytics.

64. Partant, la formation restreinte considère que le dépôt de ces cookies est soumis au recueil préalable du consentement de l'utilisateur, dès lors qu'ils n'ont pas pour finalité exclusive de permettre ou de faciliter la communication par voie électronique et ne sont pas non plus strictement nécessaires à la fourniture d'un service expressément demandé par l'utilisateur.

65. En conséquence, la formation restreinte considère qu'en permettant le dépôt et la lecture du cookie Google Analytics sur le terminal des personnes lors de leur arrivée sur le site web www.neosurf.com, sans recueillir préalablement leur consentement, la société a privé celles-ci de la possibilité, qui leur est accordée par l'article 82 de la loi Informatique et Libertés, d'exercer un choix quant au dépôt de traceurs sur leur équipement terminal.

66. La formation restreinte relève que la société a démontré au cours de la procédure, que depuis le 16 août 2023, plus aucun cookie Google Analytics n'est déposé sur le terminal des utilisateurs. Elle rappelle néanmoins que les mesures de mises en conformité adoptées ne sauraient exonérer la société de sa responsabilité pour le passé.

2. Sur l'utilisation du mécanisme de reCaptcha Google sans recueil du consentement de l'utilisateur

67. Le rapporteur relève que la société utilisait le module Google reCaptcha, dans le but de bloquer les robots sur la page d'inscription et de connexion au site web et à l'application mobile neosurf. Il considère que l'utilisation de module sans recueil préalable du consentement de l'utilisateur est contraire à l'article 82 de la loi Informatique et Libertés, dans la mesure où il ne relève d'aucune des exemptions prévues par cet article.

68. En défense, la société ne conteste pas les faits décrits par le rapporteur, mais indique avoir remédié aux carences constatées dans le rapport, en soumettant l'utilisation du reCaptcha au consentement préalable de l'utilisateur et en ne déposant aucun cookie ou traceur sur son terminal en cas de refus. La société ajoute que le reCaptcha de GOOGLE a été définitivement remplacé par une autre solution à la fin du mois d'octobre 2023. Elle estime toutefois qu'au vu de l'information peu lisible et peu accessible fournie par la société GOOGLE s'agissant des conséquences liées à l'utilisation du service reCaptcha, il serait inéquitable de faire peser des manquements à l'article 82 de la loi Informatique et Libertés sur ses entreprises clientes, sans tenir compte du manque de transparence et d'accessibilité des informations contractuelles fournies par la société GOOGLE, déjà condamnée par la CNIL pour ces motifs (CNIL n°SAN-2019-001 du 21 janvier 2019 et n°SAN-2021-023 du 31 décembre 2021). En conséquence, elle sollicite une révision à la baisse du montant d'amende proposé.

69. En l'espèce, la formation restreinte constate qu'un mécanisme de reCaptcha, fourni par la société GOOGLE, est utilisé lors de la création d'un compte et de la connexion au site web et à l'application mobile neosurf. Elle considère que c'est bien l'éditeur du site - en l'espèce NS CARDS FRANCE - qui a choisi de recourir au mécanisme de reCaptcha et a donc permis les actions de lecture et d'écriture des informations présentes sur les terminaux des utilisateurs.

70. Au regard de ces éléments, la formation restreinte considère que la société n'est pas fondée à soutenir qu'il serait inéquitable de faire peser sur les entreprises clientes de GOOGLE, dont elle fait partie, des manquements à l'article 82 de la loi Informatique et Libertés, en invoquant le manque de transparence et d'accessibilité des conditions contractuelles de GOOGLE. En effet, la formation restreinte considère qu'en sa qualité d'entreprise utilisatrice du service de reCaptcha de Google, la société est également responsable du respect des dispositions de la loi Informatique et Libertés lors de l'utilisation de ce mécanisme.

71. En second lieu, la formation restreinte considère que si un responsable de traitement peut se prévaloir d'une exemption à l'information et au recueil du consentement lorsque les opérations de lecture/écriture effectuées dans le terminal d'un utilisateur ont pour seule finalité la sécurisation d'un mécanisme d'authentification au bénéfice des utilisateurs (v. en ce sens, CNIL, FR, Délibération n° SAN-2021-013, précitée), il en va autrement lorsque ces opérations poursuivent également d'autres finalités qui ne sont pas strictement nécessaires à la fourniture d'un service. Or, le mécanisme de reCaptcha Google n'a pas pour seule finalité la sécurisation du mécanisme d'authentification au bénéfice des utilisateurs mais permet par ailleurs des opérations d'analyse de la part de Google, ce que la société GOOGLE précise elle-même dans ses conditions générales d'utilisation.

72. La formation restreinte relève que la société GOOGLE informe les sociétés ayant recours à la technologie reCaptcha, dans des conditions générales d'utilisation disponibles en ligne, que le fonctionnement de l'API reCAPTCHA repose sur la collecte d'informations matérielles et logicielles (telles que les données sur les appareils et les applications) et que ces données sont transmises à Google pour analyse. La société GOOGLE précise également qu'il incombe à ces sociétés d'informer les utilisateurs et de demander leur autorisation pour la collecte et le partage des données avec GOOGLE.

73. Il ressort de ces éléments que la société NS CARDS FRANCE aurait dû recueillir le consentement des utilisateurs à l'utilisation du reCaptcha, ce qui n'était pas le cas en l'espèce.

74. Au vu de ce qui précède, la formation restreinte considère qu'en recourant au mécanisme de reCaptcha fourni par la société GOOGLE sans recueillir leur consentement, la société a méconnu les dispositions de l'article 82 de la loi Informatique et Libertés. La formation restreinte prend note, ainsi que cela a été confirmé lors de l'audience, que la société NS CARDS FRANCE n'utilise plus cette technologie depuis la fin du mois d'octobre 2023. Cependant, à la date des contrôles, ce mécanisme était bien utilisé, sans consentement préalable des utilisateurs.

III. Sur les mesures correctrices et leur publicité

75. Aux termes du III de l'article 20 de la loi 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 également, le cas échéant après lui avoir adressé l'avertissement prévu au I du présent article ou, le cas échéant en complément d'une mise en demeure prévue au II, saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes : […] 7° À l'exception des cas où le traitement est mis en œuvre par l'État, une amende administrative ne pouvant excéder 10 millions d'euros ou, s'agissant d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Dans les hypothèses mentionnées aux 5 et 6 de l'article 83 du règlement (UE) 2016/679 du 27 avril 2016, ces plafonds sont portés, respectivement, à 20 millions d'euros et 4 % dudit chiffre d'affaires. La formation restreinte prend en compte, dans la détermination du montant de l'amende, les critères précisés au même article 83. "

76. L'article 83 du RGPD prévoit que " Chaque autorité de contrôle veille à ce que les amendes administratives imposées […] soient, dans chaque cas, effectives, proportionnées et dissuasives ", avant de préciser les éléments devant être pris en compte pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de cette amende.

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

1. Sur le prononcé d'une amende administrative

77. En défense, la société considère que l'amende administrative proposée est disproportionnée par rapport aux manquement allégués et à sa conduite puisqu'elle a mis en œuvre plusieurs mesures correctives, en particulier, l'application effective de sa politique de conservation des données de comptes utilisateurs, la mise en place d'une politique de mot de passe présentant un niveau de sécurité adéquat, l'utilisation d'un algorithme de hachage de mot de passe conforme à l'état de l'art et le recueil du consentement au dépôt de cookies et traceurs lorsqu'il est requis. S'agissant de ce dernier manquement, elle estime inéquitable de rechercher la responsabilité des seuls éditeurs lorsqu'en réalité, la politique répressive de la CNIL cherche à faire obstacle à l'utilisation de certains outils tels que ceux proposés par la société GOOGLE. En outre, elle souligne avoir pleinement coopéré avec les services de la CNIL. Enfin, elle considère que l'amende de 200 000 euros proposée par le rapporteur équivaut à 1,8 % de son chiffre d'affaires 2020 et est par conséquent excessive.

78. La formation restreinte rappelle qu'elle doit tenir compte, pour le prononcé d'une amende administrative, 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 affectées, 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 et dans certain cas, le niveau de dommage subi par les personnes.

79. La formation restreinte relève d'abord que les manquements reprochés à la société portent atteinte à des principes fondamentaux prévus par le RGPD et concernent de nombreuses personnes.

80. S'agissant du manquement au principe de limitation de la durée de conservation des données à caractère personnel, la société a fait preuve de négligence, en se bornant à inactiver les comptes utilisateurs qu'elle conservait au lieu d'anonymiser ou de supprimer les données qu'ils contenaient. Quoi qu'il en soit, à la supposer appliquée, la durée de conservation de dix ans déclarée lors des contrôles n'était assortie d'aucun tri entre les données à conserver et celles à supprimer, comme l'a confirmé la société lors de l'audience. La formation restreinte relève que ce manquement concerne potentiellement un nombre important de personnes, la société revendiquant environ 700 000 utilisateurs disposant d'un compte à la date des contrôles.

81. S'agissant du manquement à l'obligation d'information des personnes concernées et à la transparence, la formation restreinte relève que la société a manqué à l'exigence de fourniture d'une information complète et transparente aux personnes concernées, qui constitue pourtant un préalable indispensable à ce type de traitement de données à caractère personnel.

82. S'agissant du manquement à l'obligation d'assurer la sécurité des données à caractère personnel, la formation restreinte souligne le nombre de manquements constatés aux obligations élémentaires de sécurité, à savoir, le recours à un mot de passe insuffisamment robuste pour des comptes utilisateurs contenant pour certains des coordonnées bancaires et le hachage des mots de passe au moyen d'une fonction obsolète. La formation restreinte estime, à l'instar du rapporteur, que l'accumulation de ces défauts de sécurité par une société proposant des solutions de paiement en ligne et collectant des catégories de données hautement personnelles, a contribué à accentuer le fait que lesdites données n'ont pas suffisamment bénéficié de la protection offerte par le RGPD.

83. S'agissant du manquement relatif aux cookies déposés sur le terminal de l'utilisateur lors de la visite du site web de la société, la formation restreinte considère que l'absence de recueil du consentement a concerné chacune des personnes

qui ont visité le site web en question, soit nécessairement plusieurs centaines de milliers personnes, compte tenu du fait que la société revendiquait environ 328 186 visiteurs uniques de son site web entre les mois de septembre 2020 et septembre 2021. Elle relève également que le recours au module reCaptcha de Google sans recueil préalable du consentement de l'utilisateur concernait au moins potentiellement les 700 000 titulaires de comptes à la date des contrôles.

84. Enfin, tout en tenant compte de ce que la société a mis en place des mesures à la suite de la notification du rapport de sanction, la formation restreinte relève que ces actions n'exonèrent pas la société de sa responsabilité pour les manquements constitués pour le passé.

85. En conséquence, la formation restreinte considère qu'il y a lieu de prononcer une amende administrative pour les manquements aux articles 5- 1-e), 12, 13 et 32 du RGPD et 82 de la loi Informatique et Libertés.

2. Sur le montant de l'amende administrative

86. La formation restreinte relève d'abord que les manquements aux articles 5-1-e), 12 et 13 du RGPD constituent des manquements à des principes clés du RGPD susceptibles 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.

87. La formation restreinte rappelle ensuite que les amendes administratives doivent être à la fois effectives, proportionnées et dissuasives. Elle souligne que la société NS CARDS FRANCE a réalisé, en 2020, un chiffre d'affaires d'environ […] euros pour un résultat net de […] euros. La formation restreinte prend note de ce que le rapporteur a écarté le manquement relatif au partage des comptes d'accès à la base de données et de ce que la société ne conteste pas les autres manquements visés dans le rapport.

88. Dès lors, au regard de la responsabilité de la société, de ses capacités financières et des critères pertinents de l'article 83 du Règlement, la formation restreinte estime qu'une amende administrative d'un montant de 90 000 (quatre-vingt-dix mille) euros pour les manquements aux articles 5-1-e), 12, 13 et 32 du RGPD et une amende administrative d'un montant de 15 000 (quinze mille) euros pour les manquements à l'article 82 de la loi Informatique et Libertés, apparaissent justifiées.

B. Sur la publicité

89. La société conteste la proposition du rapporteur de rendre publique la présente délibération, en invoquant notamment la protection des secrets d'affaires dont relèveraient ses obligations contractuelles au titre du contrat conclu avec l'établissement émetteur de monnaie électronique.

90. La formation restreinte considère que la publicité de la présente décision se justifie au regard de la gravité des manquements en cause et du nombre de personnes concernées. Elle considère également que la publicité de la sanction permettra notamment d'informer l'ensemble des personnes concernées par les manquements. Enfin, s'agissant de l'argument lié à la divulgation de secret d'affaires, elle rappelle que les informations relevant des secrets d'affaires sont occultées de ses décisions publiées.

91. Enfin, la mesure est proportionnée dès lors que la décision n'identifiera plus nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.

PAR CES MOTIFS

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

• prononcer à l'encontre de la société NS CARDS FRANCE une amende administrative d'un montant de quatre-vingt-dix mille euros (90 000 €) pour manquements aux articles 5-1-e), 12, 13 et 32 du règlement (UE) n° 2016/679 du 27 avril 2016 relatif à la protection des données ;

• prononcer à l'encontre de la société NS CARDS FRANCE une amende administrative d'un montant de quinze mille euros (15 000 €) pour manquement à l'article 82 de la loi du 6 janvier 1978 modifiée ;

• 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

Alexandre LINDEN

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