Le : 05/08/2020

Date de publication sur legifrance: 05/08/2020

Commission Nationale de l'Informatique et des Libertés

Délibération n°SAN-2020-003 du 28 juillet 2020
Délibération de la formation restreinte n°SAN-2020-003 du 28 juillet 2020 concernant la société SPARTOO SAS

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

Vu la Convention no 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

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

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

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

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

Vu la décision n° 2018-076C du 30 mars 2018 de la présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification des traitements mis en œuvre par cet organisme ou pour le compte de la société SPARTOO ;

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 avril 2019 ;

Vu le rapport de Monsieur Bertrand du MARAIS, commissaire rapporteur, notifié à la société SPARTOO le 23 septembre 2019 ;

Vu les observations écrites versées par la société SPARTOO le 24 octobre 2019 ;

Vu la réponse du rapporteur à ces observations notifiée le 7 novembre 2019 au conseil de la société ;

Vu les nouvelles observations écrites du conseil de la société SPARTOO reçues le 22 novembre 2019 ainsi que les observations orales formulées lors de la séance de la formation restreinte, le 28 novembre 2019 ;

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte du 28 novembre 2019 :

- Monsieur Bertrand du MARAIS, commissaire, entendu en son rapport ;

En qualité de représentants de la société SPARTOO :

- […] ;

La société SPARTOO ayant eu la parole en dernier ;

La formation restreinte a adopté la décision suivante :

I. Faits et procédure

1. La société SPARTOO SAS (ci-après la société) est une société par actions simplifiée créée en 2006, spécialisée dans le secteur de la vente à distance de chaussures, dont le siège social est situé 16 rue Henri Barbusse, à Grenoble (38100).

2. En 2018, la société SPARTOO SAS a réalisé un chiffre d'affaires net de plus de […] d'euros et un résultat net négatif de près de […] euros. La même année, le groupe SPARTOO, comprenant la société SPARTOO SAS et ses filiales, a réalisé un chiffre d'affaires net d'environ […] d'euros et un résultat net négatif d'environ […] d'euros. Le groupe SPARTOO emploie environ 1000 salariés.

3. La société édite, pour les besoins de son activité, seize sites web au sein de treize pays de l'Union européenne, à savoir la France, l'Espagne, l'Allemagne, l'Italie, les Pays-Bas, la Slovaquie, le Danemark, la Pologne, la Suède, la Finlande, la Belgique, la République tchèque et la Hongrie ainsi qu'au Royaume-Uni. Deux autres sites web (spartoo.eu) et (spartoo.net) sont destinés à des consommateurs provenant d'autres pays et payant en euros et en dollars.

4. Le 31 mai 2018, en application de la décision no 2018-076C de la Présidente, une délégation de la Commission nationale de l'informatique et des libertés (ci-après la CNIL ou la Commission) a procédé à une mission de contrôle dans les locaux de la société SPARTOO. Cette mission a eu pour objet de vérifier le respect par cette société de l'ensemble des dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après le Règlement ou le RGPD) et de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (ci-après la loi du 6 janvier 1978 modifiée ou la loi Informatique et Libertés). Le contrôle a porté plus particulièrement sur les traitements de données à caractère personnel des clients et des prospects de la société, ainsi que sur l'enregistrement des conversations téléphoniques entre les clients et les salariés du service client de la société.

5. Au cours de cette mission de contrôle, la délégation a été informée que la société met en œuvre un traitement visant à lutter contre la fraude et les impayés, lors des paiements effectués sur ses sites web. Lorsque le protocole 3DSecure n'est pas validé, un courrier électronique est envoyé à la personne à l'origine de la commande afin qu'elle envoie des justificatifs de domicile et un scan du recto de sa carte bancaire. La société a, en outre, indiqué à la délégation qu'aucune durée de conservation des données à caractère personnel n'avait été définie et qu'elle ne procédait à aucun effacement régulier des données relatives aux clients et aux prospects à l'issue d'une période définie.

6. La délégation a constaté que dans le cadre de l'enregistrement des conversations téléphoniques passées entre les conseillers clientèles et les clients, les personnes appelant la société pouvaient s'opposer à l'enregistrement des appels téléphoniques en appuyant sur une touche de leur téléphone.

7. Enfin, la délégation a constaté que lors de la création d'un compte par un utilisateur, sur le site internet de la société, les mots de passe composés de six chiffres, contenant un seul type de caractère, étaient acceptés. La société a également indiqué que les mots de passe des comptes étaient conservés en base de production sous forme hachée au moyen de la fonction de hachage MD5, à l'aide d'un sel présent directement dans le champ de la base de données relatif aux mots de passe correspondants.

8. Par ailleurs, à l'issue du contrôle, la société a transmis à la Commission, par courriel du 7 juin 2018, les pièces complémentaires sollicitées et notamment un décompte effectué en base de données relatif au nombre de clients et de prospects ne s'étant pas connectés, depuis 2008, à ses sites internet diffusés dans les différents pays dans lesquels elle est présente. Les éléments suivants ont été fournis par la société :

- 118 768 clients dont les données personnelles étaient présentes en base ne s'étaient pas connectés depuis le 25 mai 2008 ;

- 682 164 clients ne s'étaient pas connectés depuis le 25 mai 2010 ;

- 3 620 401 clients ne s'étaient pas connectés depuis le 25 mai 2013 ;

- 5 790 121 clients ne s'étaient pas connectés depuis le 25 mai 2015 ;

- 25 911 675 prospects étaient sans activité depuis le 25 mai 2015.

9. Il ressortait également de ce décompte que la société SPARTOO détenait plus de 11 millions de comptes clients et plus de 30 millions de prospects.

10. En outre, la société a fourni à la CNIL, par courriel du 27 juin 2018, la nouvelle politique de protection des données de ses différents sites web.

11. Conformément à l'article 56 du RGPD, la CNIL a informé le 27 juillet 2018 l'ensemble des autorités de contrôle européennes de sa compétence pour agir en tant qu'autorité de contrôle chef de file concernant le traitement transfrontalier effectué par la société et ouvrant la procédure pour la déclaration des autorités concernées sur ce cas.

12. Aux fins d'instruction de ces éléments, la présidente de la Commission a désigné Monsieur Bertrand du MARAIS en qualité de rapporteur, le 18 avril 2019, sur le fondement de l'article 47 de la loi du 6 janvier 1978 modifiée dans sa version applicable au jour de la désignation.

13. Par courrier du 17 mai 2019, la société a été convoquée par le rapporteur à une audition, le 19 juin suivant, en application de l'article 74 du décret n° 2005-1309 du 20 octobre 2005 modifié.

14. À l'issue de son instruction, le rapporteur a fait notifier par huissier de justice à la société SPARTOO SAS, le 23 septembre 2019, un rapport détaillant les manquements au RGPD qu'il estimait constitués en l'espèce.

15. Ce rapport proposait à la formation restreinte de la Commission de prononcer une injonction de mettre en conformité le traitement avec les dispositions des articles 5-1-c), 5-1 e), 13, 32 et 35-1 du Règlement, assortie d'une astreinte à l'issue d'un délai de trois mois suivant la notification de la délibération de la formation restreinte, ainsi qu'une amende administrative. Il proposait également que cette décision soit rendue publique et ne permette plus d'identifier nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.

16. Était également jointe au rapport une convocation à la séance de la formation restreinte du 28 novembre 2019 indiquant à la société qu'elle disposait d'un délai d'un mois pour communiquer ses observations écrites.

17. Le 23 octobre 2019, par l'intermédiaire de son conseil, la société a produit des observations. Le rapporteur y a répondu le 7 novembre suivant.

18. Le 22 novembre, la société a produit de nouvelles observations en réponse à celles du rapporteur.

19. La société et le rapporteur ont présenté des observations orales lors de la séance de la formation restreinte du 28 novembre 2019.

20. Le projet de décision adopté par la formation restreinte a été transmis aux autorités de contrôle européennes concernées, le 16 février 2020, conformément à l'article 60.4 du Règlement général sur la protection des données (RGPD). La formation restreinte s'est prononcée, dans son projet de décision, sur les manquements proposés par le rapporteur et débattus par les parties dans le cadre du respect du principe du contradictoire, à savoir les manquements aux articles 5-1-c), 5-1 e), 13, 32 et 35-1 du RGPD ; aucun manquement à l'article 6 du RGPD et à la directive 2002/58/CE du Parlement et du Conseil dite directive ePrivacy n'ayant été soulevé par le rapporteur.

21. Les 13 et 17 mars suivants, les autorités de contrôle italienne, portugaise et de Basse-Saxe ont formulé des objections pertinentes et motivées à l'égard du projet de décision. La formation restreinte a décidé de modifier son projet de décision afin de tenir compte de ces objections. Celles-ci ne proposant pas de s'écarter du projet de décision par la prise en compte d'une circonstance de fait nouvelle, d'ajouter un manquement ou d'aggraver la nature de la mesure correctrice initialement proposée, la formation restreinte a décidé de ne pas les communiquer au rapporteur ni à la société SPARTOO.

22. Le projet de décision révisé a été soumis aux autorités de contrôle concernées le 25 juin 2020.

II. Motifs de la décision

A. Sur le manquement au principe de minimisation des données (obligation de veiller à l'adéquation, à la pertinence et au caractère non excessif des données)

23. L'article 5-1 c) du Règlement dispose que les données à caractère personnel doivent être *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) .*

24. **En premier lieu**, le rapporteur soutient que l'enregistrement intégral et permanent des appels téléphoniques reçus par les salariés du service client apparaît excessif au regard de la finalité d'évaluation de ceux-ci par la société.

25. La société soutient que les enregistrements téléphoniques ne sont ni permanents ni systématiques dans la mesure où les clients ont la possibilité de s'opposer à l'enregistrement de l'appel. Elle considère également que l'enregistrement intégral des conversations téléphoniques est proportionné aux objectifs d'évaluation et de formation des salariés poursuivis par la société. Enfin, elle soutient que c'est à tort que le rapporteur affirme que l'enregistrement des appels téléphoniques serait excessif au motif que la personne chargée d'effectuer la formation n'écoute généralement qu'un enregistrement par semaine, par salarié, alors que cette moyenne serait, selon la société, susceptible d'évoluer en fonction des besoins de l'entreprise. Elle précise que le nombre d'enregistrements que le formateur doit être à même d'écouter doit être plus important que le nombre d'enregistrements qu'il écoute effectivement.

26. La formation restreinte relève, tout d'abord, que si certains clients s'opposent à l'enregistrement de l'appel téléphonique passé, la société met en en œuvre un traitement permettant d'enregistrer toutes les conversations téléphoniques de ses salariés, sans que ceux-ci aient la possibilité de s'y opposer. Ensuite, elle considère que la société ne justifie pas de la nécessité d'enregistrer l'intégralité des conversations téléphoniques passées par le service client, au regard de la finalité du traitement, à savoir la formation des salariés. La formation restreinte relève que la société indiquait, lors de l'audition du 19 juin 2019, que la personne chargée de cette formation n'écoute généralement qu'un enregistrement par semaine et par salarié. Par ailleurs, si la société a affirmé, lors de la séance du 28 novembre 2019, que le taux d'enregistrement des conversations téléphoniques est passé de 100% à 30%, elle ne produit sur ce point aucune pièce

justificative.

27. Si le nombre d'enregistrements peut varier en fonction de chaque salarié et des circonstances, en particulier des besoins de formation de celui-ci, la formation restreinte considère que la société ne démontre pas avoir mis en place, pour le passé et l'avenir, un enregistrement des conversations téléphoniques des salariés limité à ce qui est nécessaire au regard de la finalité poursuivie. Or, un responsable de traitement ne peut mettre en place un traitement de données à caractère personnel sans s'assurer que celui-ci est nécessaire à ses besoins, *a fortiori* lorsqu'il repose sur un dispositif particulièrement intrusif pour les salariés.

28. La formation restreinte considère donc, au vu de ces éléments, qu'un manquement à l'article 5-1-c) du RGPD est constitué.

29. **En second lieu**, le rapporteur reproche à la société de ne pas avoir mis en place de mesure permettant d'éviter l'enregistrement des coordonnées bancaires des clients lors des appels téléphoniques passés avec la société. Il considère également que la mesure proposée par la société, à la suite de l'audition, consistant à supprimer chaque jour les appels en lien avec les commandes passées par téléphone avec un paiement par carte bancaire, reste insatisfaisante en ce que le traitement des données bancaires pendant une journée n'est pas justifié au regard de la finalité du traitement, qui est l'évaluation des salariés. Il rappelle que le traitement des coordonnées bancaires vise à effectuer le paiement et que de telles données n'ont pas à être enregistrées par la société, même pendant une seule journée, une fois le paiement validé.

30. La société soutient que l'effacement des données bancaires enregistrées lors des conversations téléphoniques, tous les jours, mis en place à la suite de l'audition du 19 juin 2019, permet d'assurer une conservation des données conforme au principe de minimisation. Elle précise que la mise en place d'une mesure permettant d'interrompre un enregistrement lors de la communication des coordonnées bancaires d'un client demanderait le développement d'outils techniques complexes et ferait peser un coût financier et humain particulièrement lourd.

31. La formation restreinte observe que la société a, au moins jusqu'au 19 juin 2019, enregistré à l'occasion de l'enregistrement des conversations des salariés à des fins de formation, les coordonnées bancaires des clients qui passaient des commandes par téléphone et conservé de telles données dans sa base, en clair, pendant quinze jours.

32. Elle relève que les coordonnées bancaires sont des données qui compte tenu de leur nature et des risques de fraude associés doivent faire l'objet d'une protection renforcée de la part des responsables de traitement. En effet, ainsi que l'a relevé le rapporteur, leur utilisation par des tiers non autorisés, dans le cadre de paiement frauduleux, est susceptible d'entraîner un préjudice pour les personnes concernées.

33. La formation restreinte constate que la société enregistrait et conservait des données dont elle n'avait aucun usage au regard de la finalité poursuivie par le traitement en cause, à savoir la formation des salariés.

34. Elle considère donc, au vu de ces éléments, qu'un manquement à l'article 5-1-c) du RGPD est constitué.

2. Les données collectées dans le cadre de la lutte contre la fraude

35. **En premier lieu**, le rapporteur soutient que la société méconnaît le principe de minimisation des données dès lors qu'elle conserve, dans le cadre de la lutte contre la fraude, des justificatifs envoyés par les clients tels que la copie de la carte nationale d'identité, qui ne sont pas requis.

36. La société soutient que la conservation d'un document transmis spontanément par une personne n'est pas excessive. Elle considère qu'elle peut conserver les copies de la carte nationale d'identité des personnes transmises spontanément dans la mesure où la CNIL indique

dans son guide pratique les achats en ligne qu'un responsable de traitement peut demander un justificatif d'identité et/ou de domicile pour s'assurer de l'identité du détenteur.

37. La formation restreinte note que la société a informé la CNIL, lors de l'audition du 19 juin 2019, qu'elle demandait aux clients situés en France, à des fins de lutte contre la fraude, la fourniture de la copie d'un justificatif de domicile ainsi qu'un scan de leur carte bancaire. Elle a cependant indiqué à la Commission que même si elle ne demande pas la fourniture de la copie de la carte d'identité, il arrive que les personnes lui communiquent un tel document et que dans une telle hypothèse, elle conserve ce document pendant six mois, au même titre que les autres pièces justificatives qui lui sont adressées.

38. La formation restreinte relève que la copie de la carte d'identité peut constituer un justificatif pertinent dans le cadre de la lutte contre la fraude. Par conséquent, au vu de la finalité du traitement mis en œuvre par la société et du caractère résiduel du nombre de copies de cartes d'identité traitées par la société, elle considère qu'il n'y a pas lieu de retenir, en l'espèce, le manquement reproché.

39. **En second lieu**, le rapporteur soulevait dans son rapport que la société collectait, en Italie, dans le cadre de la lutte contre la fraude la copie de la carte de santé (*tessera sanitaria*) et de la carte d'identité en cours de validité. Il reprochait à la société de ne pas avoir été en mesure d'indiquer lors de l'audition en quoi la collecte de ce document est nécessaire dans le cadre de la lutte contre la fraude. Par la suite, le rapporteur a pris acte des informations fournies par la société en vertu desquelles elle indiquait que ses déclarations faites lors de l'audition du 19 juin 2019 étaient fausses et qu'elle ne demandait en réalité aux clients que la communication de leur carte d'identité à l'exclusion de tout autre justificatif. Celle-ci a également indiqué qu'à la suite d'une erreur de communication, le service commercial de la société a demandé, entre le 27 juin et le 18 juillet 2019, aux clients la transmission de la copie de cette carte de santé, mais que cette pratique a cessé et que les documents ainsi collectés ont été supprimés. Le rapporteur a donc considéré qu'il n'y avait plus lieu de tenir compte de ce fait à l'appui du manquement précité.

40. La formation restreinte relève que la carte de santé italienne contient un nombre important d'informations sur son détenteur, à savoir son nom, prénom, genre, code fiscal, lieu de naissance correspondant pour les citoyens nés en Italie à la commune de naissance et pour les étrangers au pays de naissance. Il peut également être déduit de la date d'expiration de la carte que la personne dispose d'une autorisation de séjour en Italie.

41. Elle considère que la communication de deux documents permettant de justifier de l'identité de la personne à des fins de lutte contre la fraude, à savoir la carte de santé et la pièce d'identité, était excessive et non pertinente au titre de l'article 5-1 c) du RGPD. Il apparaît en effet que seule la collecte de la carte d'identité était pertinente au regard de la finalité du traitement mis en œuvre. En l'espèce, la collecte de la carte de santé contenant davantage d'informations que la carte d'identité, non pertinentes dans le cadre de la lutte contre la fraude, était excessive. À cet égard, la formation restreinte relève que la société reconnaît qu'une telle collecte n'était pas nécessaire, celle-ci ayant cessé en juillet 2019. La formation restreinte considère que quand bien même la société n'aurait collecté un tel document que pendant une période limitée de trois semaines, de tels éléments sont constitutifs d'un manquement à l'obligation pour le responsable de traitement de ne traiter que des données adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées, en vertu du principe de minimisation des données.

42. La formation restreinte considère donc qu'un manquement à l'article 5-1 c) du RGPD est constitué pour ces faits.

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

43. L'article 5-1 e) du Règlement dispose que 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 ;*

les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation) .

44. **En premier lieu**, le rapporteur a relevé que lors du contrôle du 31 mai 2018 la société a informé la CNIL qu'aucune durée de conservation des données des clients et prospects n'avait été déterminée et qu'elle ne procédait à aucun effacement régulier ni aucun archivage de telles données à l'issue d'une période définie. Lors de l'audition du 19 juin 2019, la société a informé le rapporteur avoir fixé une durée de conservation de ces données de cinq ans, en base active, à compter de la date de dernière activité des clients et prospects, pouvant correspondre par exemple, à une connexion au compte client, à un clic dans une newsletter ou encore à l'ouverture de celle-ci.

45. Pour la détermination du nombre de clients et de prospects à prendre en considération, il convient d'inclure ceux situés au Royaume-Uni dès lors que cet Etat étant membre de l'Union européenne à l'époque des faits en cause, le RGPD est applicable. Au surplus, dans le cadre de l'accord de retrait entre l'Union européenne et le Royaume-Uni, une période transitoire a été convenue durant laquelle le droit de l'Union continue de s'appliquer au Royaume-Uni.

46. Les relevés effectués par la société, sur demande de la délégation de contrôle, permettaient d'établir que la société conservait les données de 118 768 clients ne s'étant pas connectés à leur compte depuis le 25 mai 2008, celles de 682 164 clients ne s'étant pas connectés à leur compte depuis le 25 mai 2010 et les données de 3 620 401 clients ne s'étant pas connectés à leur compte depuis le 25 mai 2013.

47. La formation restreinte en déduit qu'au moins jusqu'au comptage réalisé le 7 juin 2018 en base de données, la société conservait un nombre particulièrement important de données concernant ses clients qui ne s'étaient pas connectés à leur compte depuis plus de dix ans.

48. En outre, le fait, allégué par la société, que seule la responsable juridique ait accès aux données des clients conservées est en tout état de cause dépourvu de portée, la durée de conservation étant indépendante de l'accès.

49. S'agissant des prospects, le rapporteur considère que la société ne justifie pas de la nécessité d'appliquer une durée de conservation de leurs données pendant cinq ans à compter du dernier contact émanant de ceux-ci.

50. La société soutient, quant à elle, que la durée de conservation de cinq ans de telles données est adéquate compte tenu de la spécificité de sa plateforme d'e-commerciale généraliste. Il serait, en outre, établi que certains prospects se connectent pour regarder les offres proposées après une période d'inactivité de quatre ans.

51. La formation restreinte note que la société conservait en juin 2018, s'agissant des différents pays de l'Union européenne dans lesquels la société exerce son activité et du Royaume-Uni, les données de plus de 25 millions de prospects n'ayant eu aucune activité depuis le 25 mai 2015, soit depuis plus de trois ans. De plus, à titre d'exemple significatif, étaient conservées les données de 4 801 596 prospects n'ayant aucune activité depuis plus de trois ans, concernant l'Espagne, celles de 5 616 503 prospects concernant l'Italie et celles de plus de 12 millions de prospects concernant la France. La formation restreinte relève qu'après avoir indiqué aux services de la CNIL que les données étaient conservées sans limitation de durée, la société a indiqué, lors de l'audition, qu'elle conserve désormais ces données pendant cinq ans à compter du dernier contact, alors même qu'elle soutient ne plus les relancer après une période d'inactivité de deux ans. La formation restreinte considère que la société n'a pas établi en quoi la conservation des données des prospects, qui sont des personnes n'ayant jamais réalisé de commande sur le site de la société ou

d'anciens clients dont les données sont utilisées à des fins de prospection après la fin de la relation commerciale, est nécessaire au-delà du délai de deux ans au cours duquel elle effectue ses opérations de prospection. La société a en effet indiqué qu'elle n'envoie des messages promouvant ses produits ou contenant des offres commerciales à ses prospects que pendant une période de deux ans.

52. Sur ce point, la formation restreinte estime qu'en l'espèce, la durée de deux ans apparaît proportionnée au vu de la finalité du traitement. Cette durée répond au souhait de la société de promouvoir, comme tout commerçant, ses produits auprès de ses anciens clients et des personnes ne s'étant pas opposées à la réception de tels messages. La société précise en outre qu'un mécanisme permet aux personnes de se désabonner à tout moment pour ne plus recevoir de messages de prospection. En revanche, la durée de conservation mise en place par la société s'agissant des données des prospects, à savoir cinq ans, excède celle nécessaire au regard des finalités pour lesquelles elles sont traitées.

53. La formation restreinte considère donc que la société a méconnu les dispositions de l'article 5-1 e) du RGPD.

54. **En deuxième lieu**, le rapporteur reproche à la société de déterminer comme point de départ du délai de conservation des données des prospects notamment l'ouverture d'un courriel de prospection.

55. La formation restreinte note que les données des prospects permettent à un responsable de traitement d'adresser des messages, par exemple par courrier électronique, à des personnes qui montrent un intérêt pour ses produits ou services. La Commission considère à cet égard que lorsque le point de départ du délai de conservation des données est le dernier contact émanant du prospect, il doit s'agir d'un évènement permettant de démontrer l'intérêt de la personne pour le message reçu, tel qu'un clic sur un lien hypertexte contenu dans un courriel. Cependant, la seule ouverture d'un courriel ne peut être considérée comme un contact émanant du prospect, dans la mesure où celui-ci peut être ouvert involontairement du fait des modalités de fonctionnement du logiciel de messagerie utilisé ou par erreur.

56. La formation restreinte considère donc que la société ne peut, sans méconnaître le principe de limitation de la durée de conservation des données, considérer que la simple ouverture d'un courriel de prospection par une personne permet de refaire courir le point de départ du délai de conservation des données des prospects et ainsi conserver de telles données alors même que les prospects n'ont pas démontré, par un acte clair, un intérêt pour les produits ou services de la société pendant plusieurs années.

57. **En troisième lieu**, le rapporteur soutient qu'à l'issue de l'expiration de la durée de conservation des données des clients, la société ne supprime pas l'intégralité des données conservées, mais conserve l'adresse électronique des clients ainsi que leurs mots de passe, sous une forme pseudonymisée, ce qui ne permettrait pas de respecter le principe de limitation de conservation des données.

58. La société soutient que *l'anonymisation* des adresses électroniques des anciens clients est effectuée à partir d'un procédé fondé sur une technologie SHA-256 et que le décryptage des données hachées avec cette fonction requiert des compétences techniques très pointues. Elle considère donc que les données des clients inactifs sont *indécryptables et donc anonymes .*

59. La formation relève qu'à l'issue de la période d'inactivité d'un client, la société supprime certaines données, à savoir les nom, prénom et date de naissance de celui-ci, mais en conserve d'autres tels que son adresse électronique et son mot de passe qui sont hachés par un algorithme et transférés au sein d'une autre table. La société souhaite ainsi permettre à un client de se reconnecter à son compte avec le même identifiant et le même mot de passe que ceux utilisées lors de la création de son compte, à l'issue de la durée de conservation des données mise en place.

60. La formation restreinte considère que les données de ses anciens clients, même hachées, ne sont pas anonymisées, mais pseudonymisées, et permettraient de réidentifier les personnes.

61. La société soutient que les adresses électroniques et les mots de passe de ses anciens clients sont hachés au moyen d'un algorithme SHA-256 qui est particulièrement robuste et qui rendrait les données anonymes.

62. La formation restreinte relève que l'algorithme SHA-256 est une fonction de hachage permettant d'assurer l'intégrité des données personnelles traitées par la société. S'il s'agit, à ce jour, d'une fonction qui ne peut être inversée et est donc considérée par l'Agence nationale de sécurité des systèmes d'information (ANSSI) et la CNIL comme garantissant un niveau de sécurité suffisant des données, celle-ci ne permet pas d'anonymiser des données et donc de justifier leur conservation de manière indéfinie par un responsable de traitement.

63. Par conséquent, la formation restreinte considère que la société conserve les données en cause pendant une durée excédant celle nécessaire au regard des finalités pour lesquelles elles sont traitées. Elle relève à cet égard, que la société indique elle-même que l'objectif de la mise en place d'une telle mesure est de permettre à ses clients de se reconnecter à leur compte, alors même que les données sont censées avoir été supprimées. Les données personnelles des anciens clients doivent être définitivement supprimées à l'issue de l'expiration du délai de conservation de celles-ci en base active ou en base archive, une fois les obligations légales expirées et ne peuvent être conservées pour une hypothétique utilisation future.

64. La formation restreinte considère donc que la société a, là encore, méconnu les dispositions de l'article 5-1 e) du RGPD.

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

65. L'article 13 du RGPD exige du responsable de traitement qu'il fournisse, au moment où les données sont collectées, les informations relatives à son identité et ses coordonnées, celles du délégué à la protection des données, les finalités du traitement et sa base juridique, les destinataires des données à caractère personnel, le cas échéant les transferts de données à caractère personnel, la durée de conservation des données à caractère personnel, les droits dont bénéficient les personnes ainsi que le droit d'introduire une réclamation auprès d'une autorité de contrôle.

66. **En ce qui concerne les clients**, le rapporteur reprochait à la société de ne pas les informer, au sein de la politique de confidentialité des données, accessible sur le site web de la société ainsi que *via* un lien présent sur le formulaire de création de compte, que leurs données sont transférées vers Madagascar, dans le cadre des appels téléphoniques. Il reprochait également à la société de ne citer au sein de ces documents qu'une seule base juridique pour tous ses traitements, à savoir le consentement, alors que certains traitements reposaient sur une base légale différente.

67. Le rapporteur relevait, dans ses observations du 7 novembre 2019, que malgré les affirmations de la société, la politique de confidentialité n'avait pas été corrigée afin d'y faire figurer le transfert de données à Madagascar.

68. S'agissant des bases juridiques du traitement, la société a affirmé qu'elle fondait ses traitements sur le consentement des personnes, ce qui, selon elle, ne pouvait lui être reproché dans la mesure où cette base légale est plus protectrice pour les personnes et que par conséquent un manquement au défaut d'information des personnes ne pouvait être retenu à son encontre en ce qui concerne ces faits.

69. La formation restreinte relève qu'il ressort des indications de la société relatives aux différents traitements mis en œuvre que plusieurs d'entre eux, à savoir, par exemple, la lutte contre la fraude ou encore ceux mis en œuvre dans le cadre des achats effectués sur le site web de la société, ne

peuvent reposer sur le consentement des personnes, mais, comme l'a indiqué le rapporteur, sur le contrat ou les intérêts légitimes poursuivis par la société. Rappelant que le considérant 41 du RGPD exige que la base légale du traitement soit *claire et précise* , elle considère que la société ne peut viser uniquement au sein de sa politique de confidentialité des données la base juridique du consentement pour l'intégralité des traitements mis en œuvre.

70. Par conséquent, si la société a effectivement, comme les textes l'exigent, intégré une information sur la base légale et eu le souci de retenir la base la plus protectrice, selon elle, des droits des personnes, la formation restreinte rappelle que l'article 13 du RGPD exige une information granulaire relative à la base juridique de chaque traitement. Elle ne peut dès lors que relever que la société ne s'est pas entièrement conformée aux dispositions de cet article en s'abstenant d'indiquer, pour chaque traitement mis en œuvre, la base légale correspondante au sein de sa politique de confidentialité.

71. Par ailleurs, la formation restreinte prend acte des modifications apportées sur son site internet, s'agissant du transfert de données à Madagascar. Elle considère cependant qu'un manquement à l'article 13 du RGPD est constitué jusqu'au 18 novembre 2019, date à laquelle la société indique avoir apporté des modifications à son site internet.

72. **En ce qui concerne les salariés**, le rapporteur reproche à la société de ne pas les informer individuellement de l'enregistrement de leurs appels téléphoniques.

73. La société soutient que les salariés sont informés de l'enregistrement des appels téléphoniques passés avec les clients, grâce à plusieurs documents, telle qu'une attestation de présence information projet écoute téléphonique datée du 14 janvier 2016, un document de mai 2014 ainsi que des fiches d'évaluation de performance datées de 2017. La société a également fourni des attestations de trois conseillers clientèles affirmant qu'ils ont pris connaissance du document daté du 14 janvier 2016, qu'ils ont compris le but de ces écoutes et qu'ils peuvent contacter le service juridique pour des informations complémentaires.

74. La formation restreinte rappelle que l'information des salariés de la mise en place de dispositifs d'écoute et d'enregistrement des conversations téléphoniques sur le lieu de travail est fondamentale et est liée au caractère loyal et transparent de tout traitement mis en œuvre par un responsable de traitement. Comme il l'est indiqué au considérant 39 du RGPD, *le principe de transparence exige que toute information et communication relatives au traitement de ces données à caractère personnel soient aisément accessibles, faciles à comprendre, et formulées en des termes clairs et simples .*

75. L'obligation de transparence oblige la société à fournir une information relative à un tel dispositif à chaque salarié, celle-ci ne pouvant se satisfaire d'une seule information, comme en l'espèce en 2016, qui ne serait pas fournie aux nouveaux salariés employés par la suite.

76. Au demeurant, la formation restreinte relève également que l'article L. 1222-4 du code du travail dispose qu' *aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance .* En outre, la Commission a rappelé à plusieurs reprises, et notamment dans un guide pour les employeurs et les salariés disponible sur son site web ainsi que dans une recommandation n° 2014-474 du 27 novembre 2014 relative à l'enregistrement des appels sur le lieu de travail, que les salariés doivent se voir fournir un certain nombre d'informations s'agissant des traitements mis en œuvre par les employeurs.

77. Enfin, la formation restreinte relève que les documents produits par la société ne permettent pas de fournir aux salariés une information relative aux finalités poursuivies par le traitement, à la base légale du dispositif, aux destinataires des données issues du dispositif, à la durée de conservation des données, à leurs droits notamment d'accès aux données les concernant ainsi qu'à la possibilité d'introduire une réclamation auprès de la CNIL, garantissant une information complète des salariés conformément à l'article 13 du RGPD.

78. La formation restreinte considère donc, au vu de ces éléments, qu'un manquement à l'article 13 du RGPD est constitué.

D. Un manquement à l'obligation d'assurer la sécurité des données

79. L'article 32-1du Règlement dispose : *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* et notamment *des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement .*

80. Le responsable du traitement doit ainsi, conformément à l'article 32-2 du RGPD, tenir compte 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.

81. La délégation de la CNIL a constaté, lors du contrôle du 31 mai 2018, que les personnes souhaitant créer un compte utilisateur sur le site web de la société pouvaient créer un mot de passe composé de six caractères comportant une seule catégorie de caractères. Lors de l'audition du 19 juin 2019, la société a précisé que, depuis le contrôle de la CNIL, une mesure de blocage d'une minute du compte a été mise en place, après 19 tentatives d'accès infructueuses à un compte à partir d'une même adresse IP en moins d'une minute.

82. En défense, la société fait valoir qu'elle a modifié les règles de constitution des mots de passe des comptes et exige désormais de ses clients qu'ils créent des mots de passe composés d'au moins huit caractères. Elle remet également en cause les préconisations de la CNIL en la matière et soutient que les recommandations techniques en termes de sécurisation des mots de passe issues de la délibération n° 2017-190 du 22 juin 2017 de la Commission font l'objet de contestations par des experts en cybersécurité. Soutenant que des règles trop complexes ont entraîné une standardisation des mots de passe, elle a préféré opter pour l'imposition de mots de passe courts et plus simples, ceux-ci étant moins prévisibles pour un éventuel attaquant, l'aléa étant basé sur une logique humaine.

83. Le rapporteur soutient que des mots de passe, composés de six ou huit caractères, sans critère de complexité, ne sont pas suffisamment robustes et ne permettent pas d'assurer la sécurité des données traitées par la société. Il considère que de tels mots de passe ne permettent pas d'empêcher des attaques par force brute qui consistent à tester successivement et de façon systématique de nombreux mots de passe et peuvent conduire, ainsi, à une compromission des comptes associés et des données personnelles qu'ils contiennent.

84. La formation restreinte considère que, contrairement à ce que soutient la société, la longueur et la complexité d'un mot de passe demeurent des critères élémentaires permettant d'apprécier la force de celui-ci. Elle rappelle que, pour assurer un niveau de sécurité suffisant et satisfaire aux exigences de robustesse des mots de passe, lorsqu'une authentification repose uniquement sur un identifiant et un mot de passe, le mot de passe doit comporter au minimum douze caractères - contenant au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial - ou le mot de passe doit comporter au moins huit caractères - contenant trois de ces quatre catégories de caractères - et être accompagné 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.

85. La formation restreinte relève que la nécessité d'un mot de passe fort est également soulignée par l'ANSSI, qui indique qu' *un bon mot de passe est avant tout un mot de passe fort, c'est à dire difficile à retrouver même à l'aide d'outils automatisés. La force d'un mot de passe dépend de sa longueur et du nombre de possibilités existantes pour chaque caractère le composant. En effet, un mot de passe constitué de minuscules, de majuscules, de caractères spéciaux et de chiffres est techniquement plus difficile à découvrir qu'un mot de passe constitué uniquement de minuscules* .

86. En l'espèce, elle considère que la robustesse d'un mot de passe composé de huit caractères et de seulement une catégorie de caractères, est très faible et que la société ne démontre à aucun moment en quoi un mot de passe court et simple serait susceptible de résister davantage à une attaque par force brute qu'un mot de passe composé de davantage de caractères ainsi que plusieurs catégories de caractères.

87. La formation restreinte considère, par conséquent, que les mots de passe mis en place par la société pour accéder aux comptes crées sur son site web ne correspondent pas aux exigences requises en termes de robustesse.

88. Il a été constaté, lors du contrôle du 31 mai 2018, que la société demande à ses clients, dans le cadre de la lutte contre la fraude, de lui transmettre par mail un scan de la carte bancaire utilisée lors de la commande. Pour ses clients en France, un courriel précisant *sur les 16 chiffres de la face avant merci de laisser apparaître au minimum les 4 premiers et les 4 derniers, la date de validité et le nom du titulaire devront apparaître clairement* est alors adressé aux personnes. Des courriels effectuant une telle demande sont également adressés aux personnes effectuant des commandes sur les sites italiens, espagnols, hongrois, slovaques, danois et grecs. il a été constaté que la société conservait les scans de cartes bancaires non occultés.

89. Le rapporteur considère ainsi que le courriel de la société adressé aux personnes, particulièrement aux français, incite à fournir une copie intégrale de la carte de paiement au lieu d'inviter les clients à cacher un minimum de numéros de leur carte bancaire.

90. Il a en outre été constaté que les scans des cartes bancaires sont conservés par la société en clair pendant six mois à compter de l'enregistrement des documents, en cas de litige.

91. Par courrier du 28 juin 2019, la société a indiqué qu'une plateforme en ligne dédiée à l'envoi des pièces justificatives serait mise en place fin août 2019. Par ailleurs, la société soutient qu'elle a été autorisée par la CNIL à mettre en œuvre un traitement ayant pour finalité la lutte contre la fraude et qu'elle peut valablement collecter les dates de fin de validité et les numéros de carte bancaire tronqués.

92. **En premier lieu**, la formation restreinte relève que la société a bien été autorisée par délibération de la CNIL du 2 juillet 2009 à traiter le numéro de carte bancaire tronqué ainsi que la date de fin de validité, dans le cadre de la mise en œuvre d'un traitement ayant pour finalité la lutte contre la fraude. Cependant, il est établi que la société traitait les copies des cartes bancaires des clients contenant l'intégralité des numéros, alors qu'elle n'était autorisée à traiter qu'une partie tronquée de ceux-ci. La formation restreinte considère donc que l'autorisation délivrée par la CNIL ne peut justifier le traitement de l'intégralité des numéros des cartes bancaire des clients.

93. **En second lieu**, la formation restreinte relève qu'il a été constaté par la délégation de la CNIL que le dispositif mis en place par la société permettait aux clients d'envoyer en clair, par courriel non chiffré à partir de leur boîte électronique, des photographies ou des scans de leur carte bancaire contenant l'intégralité du numéro de la carte bancaire et que de telles données étaient conservées, au même titre que les justificatifs demandés dans le cadre de la lutte contre la fraude, pendant six mois, en clair dans la base de données.

94. Dans ces conditions, la formation restreinte considère que la société n'a pas mis en place, au moins jusqu'en août 2019, des mesures de sécurité permettant de garantir la sécurité des données bancaires de ses clients.

95. Sur la base de l'ensemble de ces éléments, la formation restreinte considère que le manquement à l'article 32 du Règlement est constitué.

E. Sur les mesures correctrices et leur publicité

96. 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 : […]

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

7° 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.

97. L'article 83 du RGPD prévoit :

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

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

a) la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi ;

b) le fait que la violation a été commise délibérément ou par négligence ;

c) toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées ;

d) le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre en vertu des articles 25 et 32 ;

e) toute violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant ;

f) le degré de coopération établi avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs ;

g) les catégories de données à caractère personnel concernées par la violation ;

h) la manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure, le responsable du traitement ou le sous-traitant a notifié la violation ;

i) lorsque des mesures visées à l'article 58, paragraphe 2, ont été précédemment ordonnées à l'encontre du responsable du traitement ou du sous-traitant concerné pour le même objet, le respect de ces mesures ;

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

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

98. **En premier lieu**, concernant l'amende proposée par le rapporteur, la société soutient qu'elle n'a jamais été condamnée par la CNIL, qu'elle disposait de peu de référentiels avant l'entrée en application du RGPD et que la Commission avait annoncé une période de tolérance en ce qui concerne les nouveaux manquements au RGPD, tels que la minimisation ou la pseudonymisation des données.

99. La formation restreinte estime que, dans le cas d'espèce, les manquements précités justifient que soit prononcée une amende administrative à l'encontre de la société pour les motifs suivants.

100. Tout d'abord, elle constate que, contrairement à ce que soutient la société, les manquements retenus portent, pour l'essentiel, sur des obligations que la loi no 78-17 du 6 janvier 1978 modifiée imposait déjà aux responsables de traitement et qui ne sont pas nées du RGPD, y compris s'agissant du principe de minimisation et de limitation de la durée de conservation des données. Elle rappelle, en outre, que les questions relatives à la pseudonymisation des données étaient posées bien avant l'entrée en application du RGPD.

101. Ensuite, elle relève que plusieurs de ces manquements concernent des salariés et notamment leur droit à bénéficier d'une information sur les traitements de leurs données à caractère personnel. Là encore, la formation restreinte rappelle qu'il ne s'agit pas d'une nouveauté instaurée à la suite de l'entrée en application du RGPD.

102. Enfin, elle souligne que les données bancaires sont des données devant faire l'objet d'une vigilance particulière par les responsables de traitement et que la Commission n'a cessé de les accompagner sur ce sujet depuis de nombreuses années.

103. **En deuxième lieu**, la société souligne sa coopération avec le rapporteur et les mesures mises en place, ainsi que certaines sanctions précédemment prononcées par la formation restreinte. Elle considère également qu'un manque de célérité ne peut lui être reproché alors que l'audition est intervenue un an après le contrôle effectué dans ses locaux et alors qu'aucune mise en demeure ne lui a été notifiée dans ce laps de temps.

104. La formation restreinte relève que si plusieurs mesures ont été mises en place par la société afin de remédier en totalité ou en partie à certains manquements, celles-ci n'ont été adoptées qu'à la suite du contrôle de la CNIL le 31 mai 2018, en ce qui concerne la mise en place de durées de conservation des données des clients et des prospects et qu'à la suite de l'audition du 19 juin

2019, et du rapport, s'agissant de la suppression des enregistrements contenant des coordonnées bancaires des clients et l'information des personnes sur le site web relative au transfert de leurs données hors de l'Union européenne.

105. Ensuite, la formation restreinte considère que la gravité de certains manquements est caractérisée. Plus particulièrement s'agissant du manquement relatif à l'enregistrement des conversations téléphoniques, la formation restreinte relève que la société a enregistré pendant plusieurs années l'intégralité des conversations téléphoniques de ses salariés, alors même qu'elle n'en n'avait aucune utilité et qu'un tel traitement peut s'apparenter à une surveillance constante. Elle relève également que l'information des salariés quant à la mise en place du dispositif d'enregistrement des appels est particulièrement défaillante, celle-ci étant soit incomplète avant 2016, soit inexistante pour les salariés engagés par la société postérieurement.

106. Par ailleurs, la gravité des manquements est caractérisée au vu de la catégorie particulière de données à caractère personnel traitées par la société, à savoir les données bancaires qui sont considérées comme étant des données exposant les personnes à un risque de fraude, donc de préjudice, et doivent, de ce fait, faire l'objet d'une vigilance particulière. Enfin, la formation restreinte considère également que la gravité est caractérisée en raison du nombre de personnes concernées par les manquements, s'agissant notamment des durées de conservation des données, celui-ci ayant affecté plusieurs milliers de personnes.

107. La société soutient ensuite être une entreprise de taille intermédiaire et agir dans un secteur particulièrement concurrentiel. Elle considère qu'une amende administrative élevée affecterait sa santé financière et sa position commerciale.

108. À ce sujet, la formation restreinte considère que la société est un acteur établi de l'e-commerce, et que, créée bien avant l'entrée en application du RGPD, elle ne pouvait ignorer les règles de bases de la protection des données personnelles.

109. Ensuite, la formation restreinte rappelle que le § 3 de l'article 83 du Règlement prévoit qu'en cas de violations multiples, comme c'est le cas en l'espèce puisque quatre manquements sont caractérisés, le montant total de l'amende ne peut excéder le montant fixé pour la violation la plus grave. Dans la mesure où il est reproché à la société un manquement aux articles 5 et 12 du Règlement, le montant maximum de l'amende pouvant être retenu s'élève à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

110. Toutefois, la formation restreinte tient également compte, dans la détermination de l'amende prononcée, des mesures que la société a prises au cours de la procédure de sanction pour se mettre partiellement en conformité ainsi que la coopération avec les services de la Commission.

111. **En troisième lieu**, concernant la nécessité de prononcer une injonction, la société considère qu'une mise en demeure sans astreinte serait plus adaptée compte tenu de la célérité déjà constatée pour se mettre en conformité sur plusieurs manquements.

112. Sans ignorer les démarches de la société pour se mettre en conformité avec le RGPD, la formation restreinte considère que la société n'a pas démontré, au jour de la clôture de l'instruction, la conformité totale des traitements qu'elle met en œuvre aux articles 5-1-c), 5-1 e) 13 et 32 du Règlement.

113. Faute pour la société de s'être mise en conformité sur ces manquements, il y a lieu de prononcer une injonction.

114. **En quatrième lieu**, la formation restreinte considère que la publicité de la sanction se justifie au regard de l'importance des problématiques soulevées concernant les salariés, ainsi que la nature des données en cause, alors que la société est un acteur important du secteur dans lequel elle intervient.

115. Il résulte de tout ce qui précède et de la prise en compte des critères fixés à l'article 83 du RGPD qu'une amende administrative à hauteur de 250 000 euros, une injonction assortie d'une astreinte ainsi qu'une sanction complémentaire de publication pour une durée de deux ans sont justifiées et proportionnées.

PAR CES MOTIFS

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

· prononcer à l'encontre de la société SPARTOO SAS une injonction de mettre en conformité les traitements avec les obligations résultant des articles 5-1 c), article 5- 1 e), 13 et 32 du règlement no 2016/679 du 27 avril 2016 relatif à la protection des données, et en particulier :

· s'agissant du manquement au principe de minimisation des données à caractère personnel :

o justifier de la fin des enregistrements non ponctuels et non aléaloires des conversations téléphoniques des conseillers lorsque la finalité poursuivie est leur formation ou leur évaluation ;

· s'agissant du manquement au principe de limitation de la durée de conservation des données, définir et mettre en œuvre une politique de durée de conservation des données relatives aux clients et aux prospects qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées, et notamment :

o justifier de la procédure d'archivage intermédiaire des données à caractère personnel des clients mise en place, après avoir opéré un tri des données pertinentes à archiver et une suppression des données non pertinentes, ainsi que du point de départ de cet archivage ;

o justifier de la restriction des accès des salariés aux données à caractère personnel présentes en base active aux seules personnes ayant à en connaître;

o cesser de traiter les données des prospects au-delà du délai à l'issue duquel la société ne les contacte plus (en l'espèce deux ans) et cesser de prendre en compte, comme dernier point de contact émanant de ces derniers, la simple ouverture d'un courriel ;

o cesser de conserver les adresses électroniques et mots de passes hachés des anciens clients à l'issue de la période d'inactivité fixée et procéder à la purge de telles données conservées par la société jusqu'à la date de la délibération de la formation restreinte ;

o justifier de la suppression des données concernant les clients au-delà de la période d'inactivité définie, dont il appartiendra à la société de justifier, et concernant les prospects au-delà de deux ans d'inactivité ;

· s'agissant du manquement à l'obligation d'informer les personnes :

o procéder à l'information des salariés relative à la mise en place d'un dispositif d'enregistrement des conversations téléphoniques concernant notamment les finalités poursuivies, la base légale du dispositif, les destinataires des données issues du dispositif, la durée de conservation des données, les droits des salariés notamment d'accès aux données les concernant, la possibilité d'introduire une réclamation auprès de la CNIL ;

o procéder à l'information complète des clients, en fournissant une information relative aux différentes bases légales des traitements mis en œuvre par la société ;

· s'agissant du manquement à l'obligation d'assurer la sécurité des données personnelles, prendre toute mesure, pour l'ensemble des traitements de données à caractère personnel mis en œuvre, permettant de préserver la sécurité de ces données et d'empêcher que des tiers non autorisés y

aient accès en application de l'article 32 du RGPD, notamment :

o mettre en œuvre une politique de gestion des mots de passe contraignante, s'agissant des comptes clients selon l'une des modalités suivantes ;

§ les mots de passe sont composés d'au minimum douze caractères, contenant au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial ;

§ les mots de passe sont composés d'au moins huit caractères, contenant trois des quatre catégories de caractères (lettres majuscules, lettres minuscules, chiffres et caractères spéciaux) et s'accompagnent d'une mesure complémentaire comme 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) ;

· assortir l'injonction d'une astreinte de 250 (deux cent cinquante) euros par jour de retard à l'issue d'un délai de 3 (trois) mois suivant la notification de la présente délibération, les justificatifs de la mise en conformité devant être adressés à la formation restreinte dans ce délai ;

· pour les manquements aux articles 5-1 c), 5-1 e), 13 et 32 du RGPD, prononcer à l'encontre de la société SPARTOO SAS une amende administrative d'un montant de 250 000 (deux cent cinquante mille) euros ;

· 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.